

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-270785

(43) 公開日 平成9年(1997)10月14日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/14			H 0 4 L 9/00	6 4 1
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 B
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 B

審査請求 未請求 請求項の数16 O L (全 24 頁)

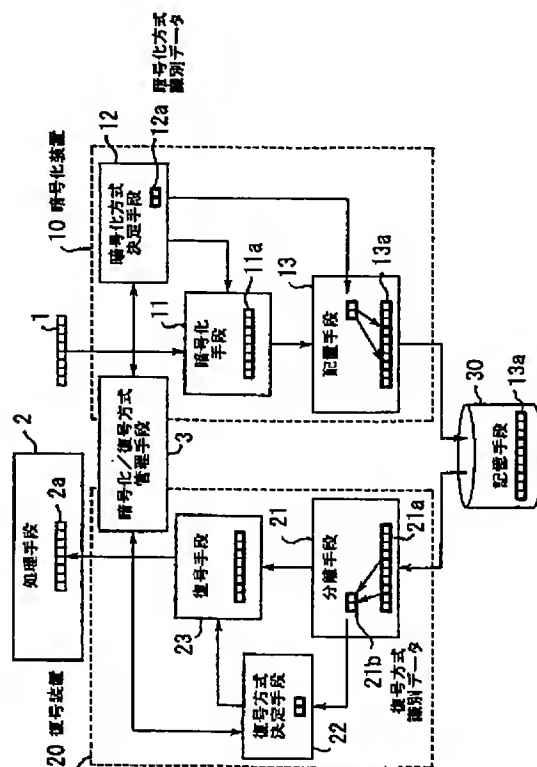
(21) 出願番号	特願平8-180453	(71) 出願人	000005496 富士ゼロックス株式会社 東京都港区赤坂二丁目17番22号
(22) 出願日	平成8年(1996)7月10日	(72) 発明者	河野 健二 神奈川県足柄上郡中井町境430 グリーン テクなかい 富士ゼロックス株式会社内
(31) 優先権主張番号	特願平8-13939	(72) 発明者	田口 正弘 神奈川県足柄上郡中井町境430 グリーン テクなかい 富士ゼロックス株式会社内
(32) 優先日	平8(1996)1月30日	(72) 発明者	齊藤 和雄 神奈川県足柄上郡中井町境430 グリーン テクなかい 富士ゼロックス株式会社内
(33) 優先権主張国	日本 (J P)	(74) 代理人	弁理士 服部 毅蔵

(54) 【発明の名称】 情報処理装置

(57) 【要約】

【課題】 コンピュータのメモリの管理方法に依存せずに、少ない計算量の暗号アルゴリズム及び簡単な鍵管理により暗号強度の高い暗号化データを得る。

【解決手段】 暗号化対象データ1は任意の暗号化方式により暗号化され暗号データ11aとなる。配置手段13により、暗号化方式を示す暗号化方式識別データ12aが暗号データ11a内に配置され、暗号データ13aが生成される。暗号データ13aは、記憶手段30に格納される。暗号データ13aのデータ処理が必要になると、分離手段21により、暗号データ13aが復号対象データ21aと復号方式識別データ21bとに分離される。復号方式決定手段22が、復号方式識別データ21bから復号方式を決定し、その復号方式により復号手段23が、復号対象データ21aを復号する。復号手段23により復号されたデータ2aは、暗号化対象データ1と同一のデータとなる。



【特許請求の範囲】

【請求項1】 入力されたデータを、識別データと暗号化対象データとに分離する分離手段と、

前記分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、

前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、

を有することを特徴とする情報処理装置。

【請求項2】 入力されたデータを暗号化する暗号化装置を有する情報処理装置において、

暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する選択手段と、

前記選択手段により選択された暗号化方式を用いて前記入力されたデータを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化手段により暗号化された暗号化データを、所定の関数に入力して関数値を計算する計算手段と、

前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記計算手段により得られた関数値に対応付けて格納する復号方式記憶手段と、
を有することを特徴とする情報処理装置。

【請求項3】 暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、

を有することを特徴とする情報処理装置。

【請求項4】 前記暗号化手段を囲む包囲体に対して外部から物理的な作用を受けると、前記暗号化手段の処理機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項1、請求項2、又は請求項3のいずれか1項に記載の情報処理装置。

【請求項5】 前記決定手段により決定される暗号化方式を変更する変更手段をさらに有することを特徴とする請求項1、請求項2、又は請求項3のいずれか1項に記載の情報処理装置。

【請求項6】 識別データが復号対象データ内の所定の位置に配置された入力データを、前記識別データと前記復号対象データとに分離する分離手段と、
前記分離手段が分離した前記識別データに応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、

前記決定手段で決定された復号方式を用いて、前記復号対象データを前記復号対象データと同ビット数に復号する復号手段と、

前記識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項7】 入力された暗号化データを復号する復号装置を有する情報処理装置において、

前記暗号化データを、所定の関数に入力して関数値を計算する計算手段と、

前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記関数値に対応付けて格納する復号方式記憶手段と、

前記計算手段により算出された関数値に対応する復号方式を前記復号方式記憶手段内から選択する復号方式選択手段と、

前記復号方式選択手段で選択された復号方式を用いて、前記暗号化データを復号する復号手段と、
を有することを特徴とする情報処理装置。

【請求項8】 前記復号手段を囲む包囲体に対して外部から物理的な作用を受けると、前記復号手段の処理機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項6又は請求項7のいずれか1項に記載の情報処理装置。

【請求項9】 前記決定手段により決定される復号方式を変更する変更手段を、さらに有することを特徴とする請求項6又は請求項7のいずれか1項に記載の情報処理装置。

【請求項10】 データの暗号化及び暗号化データの復号を行う暗号化装置及び復号装置を有する情報処理装置において、

入力されたデータを、識別データと暗号化対象データとに分離する入力データ分離手段と、

前記入力データ分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、
前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、

前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、

前記配置手段により前記識別データが配置された暗号化データを格納する記憶手段と、

前記記憶手段に格納された前記識別データが配置された暗号化データを、識別データと暗号化データとに分離する分離手段と、

前記分離手段により分離された識別データに応じて、暗号化方式に対応した復号鍵と復号アルゴリズムとの組み

合わせにより特定される復号方式を決定する復号方式決定手段と、

前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを前記暗号化データと同ビット数に復号する復号手段と、

前記復号方式決定手段による復号方式を示す識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する再配置手段と、

前記復号手段により復号されたデータの処理を行う情報処理手段と、

を有することを特徴とする情報処理装置。

【請求項 11】 データの暗号化及び暗号化データの復号を行う暗号化復号装置を有する情報処理装置において、

暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する暗号化方式選択手段と、

前記暗号化方式選択手段により選択された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化手段により暗号化された暗号化データを、特定の関数に入力して関数値を計算する第1の計算手段と、

前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記第1の計算手段により得られた関数値に対応づけて格納する復号方式記憶手段と、

前記暗号化手段により暗号化された暗号化データを格納する記憶手段と、

前記記憶手段に格納された暗号化データを、特定の関数に入力して関数値を計算する第2の計算手段と、

前記第2の計算手段により算出された関数値に対応する復号方式を、前記復号方式記憶手段内から選択する復号方式選択手段と、

前記復号方式選択手段で選択された復号方式を用いて、

前記暗号化データを復号する復号手段と、

前記復号手段により復号されたデータの処理を行う情報処理手段と、

を有することを特徴とする情報処理装置。

【請求項 12】 予め復号鍵と復号アルゴリズムとが特定されている暗号化データが入力されると、入力された暗号化データを復号する既知方式復号手段をさらに有し、

前記暗号化手段は、前記既知方式復号手段で復号されたデータも、暗号化対象データとして暗号化することを特徴とする請求項2、請求項3、請求項10、又は請求項11のいずれか1項に記載の情報処理装置。

【請求項 13】 入力された暗号化データが暗号化された際の暗号化方式と異なる暗号化方式により、前記復号手段が復号したデータを暗号化する別方式暗号化手段を、さらに有することを特徴とする請求項6、請求項

7、請求項10、又は請求項11のいずれか1項に記載の情報処理装置。

【請求項 14】 入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、

前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化する暗号化手段と、

を有することを特徴とする情報処理装置。

【請求項 15】 復号対象データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、

前記決定手段で決定された復号方式を用いて、前記復号対象データを復号する復号手段と、

を有することを特徴とする情報処理装置。

【請求項 16】 入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、

前記暗号化方式決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化手段により生成された前記暗号化データを格納する記憶手段と、

前記記憶手段内に格納された前記暗号化データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する復号方式決定手段と、

前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、

を有することを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はソフトウェアの保護機能付情報処理装置に関し、特に処理が行われたデータを逐次暗号化する暗号化装置を有するか、処理を行うべき暗号化データを逐次復号する復号装置を有するか、あるいはそれらの双方を有する情報処理装置に関する。

【0002】

【従来の技術】作成したプログラムやデータ（以下、特にことわりのない限りプログラムとデータとを含めて単に「データ」と呼ぶ）を流通させる場合、データを盗用や改ざんあるいは不正使用から保護する必要がある。これまでの保護手段としては、データをロム化したり、フロッピー等に記憶しコピープロテクトをかける等の方法がとられてきた。ところが、このような方法ではデータの内容を容易に読み出すことが可能であるためデータを完全に保護することはできない。

【0003】また、データを暗号化して流通させ、復号鍵を持ったユーザのみがデータを復号して使用できるようにすることが可能である。ただし、この方法では復号

された後のプログラムまたはデータが無防備であり、そこがセキュリティホールとなり盗用や改ざん及び不正使用を許してしまう結果となる。

【0004】これらの問題を解決する技術として、復号された後のプログラムまたはデータを不正に入手できないようにするために、データを暗号化しメモリ等に格納しておきそれを中央処理装置で実行する時に復号する方式が、特開平2-155034号の「セキュリティ機能付き情報処理装置」に示されている。この方式では、データを保護するために、情報処理装置内部に暗号化装置と復号装置とを設けており、これにより、ソフトウェアの保護を図っている。この情報処理装置について具体的に説明する。

【0005】図18は従来のソフトウェアの保護を図った情報処理装置のブロック図である。図18に示した情報処理装置は、中央処理装置510、記憶装置523、入力装置521、出力装置522、及び鍵入力装置524を備えている。さらに、中央処理装置510は、内部に演算部511、制御部512、暗号化・復号部513、及び鍵格納部514を備えている。

【0006】中央処理装置510は、情報処理装置の中心部分として機能し、データの演算や他の装置の制御等を行う。記憶装置523は、データが格納される装置であり、中央処理装置510からの制御によって中央処理装置510内の暗号化・復号部513とデータの授受を行う。

【0007】入力装置521は、中央処理装置510からの制御で情報処理装置の外部からのデータを受け取る。出力装置522は、中央処理装置510からの制御で情報処理装置のデータを外部に出力する。鍵入力装置524は、中央処理装置510の暗号化や復号を行うのに必要な鍵をセットする。

【0008】中央処理装置510内の演算部511は入力装置521や記憶装置523から与えられたデータに対して算術演算や論理演算を行う。制御部512は記憶装置523からの命令を解釈し情報処理装置全体の制御を行う。鍵格納部514は、鍵入力装置524がセットした鍵を格納する。暗号化・復号部513は記憶装置523と演算部511との間にあり、暗号化されている記憶装置523上の命令及びデータを、鍵格納部514内の鍵を用いて演算部511が解釈できるように復号するとともに、演算部511で演算された結果を記憶装置523に書き込む際に、鍵格納部514内の鍵を用いて暗号化し記憶装置523に格納する。

【0009】このような構成により、記憶装置523に格納されるデータを常に暗号化しておくことができる。そのため、記憶装置523内のデータを盗用してもその内容を解釈することは困難となり、データの秘匿性を高めることができる。

【0010】ところで、この様なソフトウェアの保護機

能が付いた情報処理装置においては、暗号化して格納されたプログラムやデータを実行時に逐次復号して実行しなければならない。そのため、復号する際のオーバーヘッドを考慮して計算量が少ない比較的簡単なアルゴリズムの暗号化方式（例えばXOR等）を用いなければならない。結果として暗号強度が低くなるという問題がある。従って、比較的簡単なアルゴリズムの暗号化方式でも暗号強度を出来るだけ高める必要がある。

【0011】そこで、情報処理装置ごとに暗号化の方法を変えて非公開にする努力がなされている。ただし、このような方法を用いるとデータの互換性が大きく失われてしまうという新たな問題が発生する。しかも、プログラム内の命令コードの出現頻度や暗号化されたプログラムと装置の動作の対応などから、暗号化アルゴリズムや暗号鍵が類推できるので、装置単位で見ると必ずしも暗号強度が高くなったとは言えない。

【0012】このように、単に暗号化の方式を非公開にするだけでは十分な暗号強度が得られないため、少ない計算量で高い暗号強度を得られるような、他の手法がいくつか考えられている。その例を、以下に説明する。

【0013】第1の例として、メモリのアドレス（エリア）ごとに暗号化アルゴリズムを変える方式がある。これは、特開昭63-184853号公報「携帯可能電子装置」に開示されている。これには、複数のエリアに分割されたデータメモリ部と、このデータメモリ部に対してデータの読み出し及びデータの書き込みを行うための制御部とを設け、データメモリ部のエリアごとに異なる暗号化アルゴリズムが割当てられている。これにより、アドレスやエリアにより暗号化アルゴリズムや暗号鍵を変えることができ、データの秘匿性がより高いものとなる。

【0014】第2の例として、メモリ内のあるアドレス上のデータによりそのデータ自身及び残りのデータ全てを暗号化する方式がある。これは、特開平4-229346号公報「プログラムコード保護用に使用すべきアドレスした情報のストリームのエンクリプション」に開示されている。この方式は、EPROM (Erasable and Programmable Read Only Memory) 内の保護されたプログラムまたはデータを開示することなしに検査または転送するためのものである。この方法によれば、暗号鍵がメモリ内のデータであるので暗号鍵を格納するキープットを特別に設ける必要がなく、EPROMのシリコン面積を無駄に使用することがない。また、暗号鍵に用いたデータ領域も自身によって暗号化されるので、例えば暗号化方法に排他的NORゲートを用いた場合には暗号鍵に用いたデータ領域が論理値1の出力バイトとなり暗号鍵を秘匿することができる。

【0015】第3の例として、複数の暗号鍵を用いる代わりにDES (Data Encryption Standard: 米商務省標準局〔現在の米国標準技術協会〕が1977年に公表し

た暗号アルゴリズム)の動作モードであるCBC (Cipher Block Chaining)やCFB (Cipher Feed Back)を用いて暗号強度を高める方式がある。これらは1つの暗号化ステップの出力を用いて次の暗号化ステップの入力を修正するものである。

【0016】DESは、暗号化の対象となるデータを64ビットのブロックに分割し、1ブロックずつ処置するが、CBCでは、ブロック毎のデータと暗号鍵だけでなく、前のブロックの暗号化によって得られる値も使用する。一方、CFBは、最初のブロックを暗号化し、それによって得られた暗号化データをDESへの入力として使用して、擬似ランダム出力を生成する。この出力をさらに次のブロックのデータに結合し暗号文を生成する。これを繰り返し、暗号文を次々に連結していく。CBCやCFBのようにすることでそれぞれの暗号ブロックは影響し合い、直前の暗号ブロックだけではなく全ての暗号ブロックを関連づけることができるので所与の順序以外では復号できないようにすることができる。

【0017】第4の例として、特開平4-101529号公報「暗号化通信方式」が公開されている。これは、暗号化した電文中に暗号鍵を挿入して伝送し、受信された暗号化電文中から前記暗号鍵を抽出し、抽出された暗号鍵を使用して前記暗号化電文を解読することを特徴とする暗号化通信方式について記載したものである。この暗号化通信方式では、暗号鍵をそのまま暗号化電文中に挿入し、暗号鍵を挿入する位置は送信先との通信回数で決まる乱数値によって決定される。送信側と受信側では、お互いに通信回数をカウントするカウンタと、そのカウンタの値に応じた乱数値を発生させる乱数発生手段を共有している。この様にすることで、暗号鍵を通信ごとに変えることができ、盗聴者による盗聴を困難にすることができる。

【0018】

【発明が解決しようとする課題】しかし、上記に示したような計算量が少なくかつ暗号強度を高めるための方式には、それぞれ次のような問題点がある。

【0019】第1の例に示したアドレスやエリアにより暗号化アルゴリズムや暗号鍵を変える方法は、ROM (Read Only Memory)のようなデータとデータアドレスの関係が変わらないようなメモリに対しては有効である。ところが、現在主流となっている仮想メモリを有するコンピュータには、この方法を適用することができない。

【0020】つまり、仮想メモリを有するコンピュータでは、プロセッサに対して記憶装置がメインメモリと補助メモリとの階層構造をなしている。この場合、暗号化されたデータが補助メモリからメインメモリへスワップインしたり、メインメモリから補助メモリへスワップアウトするたびに暗号化されたデータのメインメモリ上のアドレスが頻繁に変化する。その結果、暗号化アルゴリ

ズムまたは暗号鍵とデータアドレス上の暗号化されたデータとの整合が取れなくなるという問題が生じる。

【0021】第2の例に示した方式は、暗号化の領域がアドレスにより決定されており、第1の例に示した方式と同様にメモリの階層構造を持った記憶装置には適用できない。

【0022】第3の例に示した方式は、実質的には1つの暗号鍵しか用いていないので、その暗号鍵が露呈した場合には他の全てのデータが解読されてしまうという問題は解決されない。

【0023】第4の例に示した方式は、通信に用いる暗号化方式であり、通信側と受信側で暗号鍵を共用しないですむように、暗号鍵そのものを暗号化電文中に挿入している。従って、暗号鍵を挿入する位置が盗聴者に知られてしまうと、暗号鍵そのものが露呈してしまうという問題が生じる。それを防ぐために第4の例では、通信回数で決まる乱数値によって暗号鍵を挿入する位置を変化させてこの問題を解消させていた。従って、通信側と受信側で正確にデータをやり取りするためには、互いに同期を取る必要があり、暗号化される順番と復号される順番を同じにする必要がある。しかし、ランダムアクセスを基本とした情報処理装置のメモリにおいて、上記の方式を適用することは事実上不可能である。

【0024】また、情報処理装置で取り扱われるデータの単位は、処理の効率上同一のビット数(32ビットや64ビット)となることが多い。従って、暗号化することにより暗号鍵のビット数分データが付加されると、暗号化前と暗号化された後とはデータのサイズが変化してしまうため、それを前提にしてソフトウェアを設計しなければならず、ソフトウェアの汎用性が大きく損なわれてしまうと共に、一部暗号化方式の情報をソフトウェア開発者に公開しなければならなくなり、暗号強度が著しく低下することになる。

【0025】また、ソフトウェアの汎用性を保とうとすると、データのサイズの変化をハードウェアで補わなければならない情報処理装置のアーキテクチャの大幅な設計変更が必要となる。

【0026】さらに、情報処理装置で取り扱われるデータの単位は一般に通信の場合よりも短く、暗号化されるデータに対する暗号鍵データのサイズの割合が大きくなり記憶装置のメモリ空間を有効に活用できなくなるという問題が生じる。また、メモリ空間を浪費しないように暗号鍵データのサイズを短くすると、暗号強度が低下してしまう。

【0027】なお、第1の例に示した方式の問題点を解決する手段として、アドレスやエリアを仮想メモリ空間に対応させることにより、暗号化アルゴリズムまたは暗号鍵とアドレス上の暗号化されたデータとの整合を取ることにも可能である。ただし、このような仮想アドレスの管理はオペレーションシステム(以下、OSと呼ぶ)で

行わなければならない。一般にOSはソフトウェアであるので、特に暗号強度が低いこのようなシステムでは、OS内の暗号化アルゴリズムまたは暗号鍵の切替えを制御している部分を集中的に解読することで容易に改ざん可能である。その結果、一旦装置内部で復号したデータをそのまま外部に出力するような改ざんが可能となり、OSの一部を改ざんしただけで全てのデータが解読されるという問題が生じる。

【0028】以上のように、従来は、コンピュータのメモリの管理方法に依存せずに、少ない計算量で高い暗号強度を得ることが困難であった。なお、複数の鍵又は暗号アルゴリズムを用いた暗号方法を用いれば、少ない計算で強い暗号強度が得られるが、この場合であっても、OSの制御による複雑な鍵管理が介在しないことが条件である。

【0029】本発明はこのような点に鑑みてなされたものであり、コンピュータのメモリの管理方法に依存せずに、少ない計算量の暗号アルゴリズム及び簡単な鍵管理により暗号強度の高い暗号化データを得る暗号化装置を有する情報処理装置を提供することを目的とする。

【0030】また、本発明の他の目的は、コンピュータのメモリの管理方法に依存せずに、暗号強度の高い暗号化データを少ない計算量の復号アルゴリズム及び簡単な鍵管理で復号することができる復号装置を有する情報処理装置を提供することである。

【0031】さらに、本発明の別の目的は、コンピュータのメモリの管理方法に依存せずに、暗号強度の高い暗号化データへの暗号化とその暗号化データの復号とを、少ない計算量の暗号化／復号アルゴリズム及び簡単な鍵管理で行うことのできる暗号化／復号装置を有する情報処理装置を提供することにある。

【0032】

【課題を解決するための手段】上記課題を解決するために、第1の発明では、入力されたデータを、識別データと暗号化対象データとに分離する入力データ分離手段と、前記入力データ分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、前記配置手段により前記識別データが配置された暗号化データを格納する記憶手段と、前記記憶手段に格納された前記識別データが配置された暗号化データを、識別データと暗号化データとに分離する分離手段と、前記分離手段により分離された識別データに応じて、復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段と、前記復号方式決定手段で決定

された復号方式を用いて、前記暗号化データを復号する復号手段と、前記識別データを前記復号手段で復号されたデータ内の所定の位置に配置する再配置手段と、前記再配置手段により識別データが配置されたデータの処理を行う情報処理手段と、を有することを特徴とする情報処理装置が提供される。

【0033】この情報処理装置によれば、暗号化されているデータが識別データと暗号化データとに分離され、分離された識別データにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、入力されたデータの一部を識別データとして用いているので、復号方式を特定するために余分な情報を付加する必要がない。また、暗号鍵そのものではなく識別データを用いることによって暗号鍵のビット長に制約がなくなるとともに、暗号化アルゴリズムも複数のものを使用することが可能となる。

【0034】また、第2の発明では、暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、前記暗号化手段により暗号化された暗号化データを、所定の関数に入力して関数値を計算する第1の計算手段と、前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記第1の計算手段により得られた関数値に対応づけて格納する復号方式記憶手段と、前記暗号化手段により暗号化された暗号化データを格納する記憶手段と、前記記憶手段に格納された暗号化データを、前記第1の計算手段で用いられた関数に入力して関数値を計算する第2の計算手段と、前記第2の計算手段により算出された関数値に対応する復号方式を前記復号方式記憶手段内から選択し、復号方式を決定する復号方式決定手段と、前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、前記復号手段により復号されたデータの処理を行う情報処理手段と、を有することを特徴とする情報処理装置が提供される。

【0035】この情報処理装置によれば、暗号化データの関数値により暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。

【0036】また、第3の発明では、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、前記決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し暗号化データを生成する暗号化手段と、前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、を有することを特徴とする情報処理装置が提供される。

【0037】前記第3の発明においては、課題で述べたように暗号化した場合にデータのサイズが増加してしまうためソフトウェアを一部書き換えるか又はアーキテクチャの設計変更が必要となるが、暗号鍵そのものでなく識別データを付加しているためソフトウェア設計者に識別データのビット長を公開したとしても、暗号鍵そのもののビット長は秘密にすることができるので、暗号強度の低下を防ぐことができる。従って、この情報処理装置によれば、暗号化されているデータにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、暗号鍵そのものではなく識別データを用いることによって暗号鍵のビット長に制約がなくなるとともに、暗号化アルゴリズムも複数のものを使用することが可能となる。

【0038】また、第4の発明では、入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、前記暗号化方式決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、前記暗号化手段により生成された前記暗号化データを格納する記憶手段と、前記記憶手段内に格納された前記暗号化データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する復号方式決定手段と、前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、を有することを特徴とする情報処理装置が提供される。

【0039】第4の発明の情報処理装置によれば、パリティビットの値により暗号化方式と復号方式を決定することができるため、メモリのエリアごとの管理やアドレスごとの管理がまったく必要なくなるとともに、汎用のパリティチェック機構を暗号化方式又は復号方式の決定に利用することで、複数の暗号化方式又は復号方式の管理に必要な機構を大幅に削減することができる。

【0040】図1は本発明の情報処理装置の原理構成を示す図である。第1の発明では、暗号鍵と暗号化アルゴ

リズムとの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段12と、前記暗号化方式決定手段12により決定された暗号化方式を用いて暗号化対象データ1を暗号化し、暗号データ11aを生成する暗号化手段11と、前記暗号データ1の暗号化に用いられた暗号化方式を示す暗号化方式識別データ12aを、前記暗号データ内の所定の位置に配置する配置手段13と、前記配置手段13により暗号化方式識別データ12aが配置された暗号データ13aを格納する記憶手段30と、前記記憶手段30に格納された暗号データ13aを、復号方式識別データ21bと復号対象データ21aとに分離する分離手段21と、前記分離手段21により分離された復号方式識別データ21bに応じて、復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段22と、前記復号方式決定手段22で決定された復号方式を用いて、前記復号対象データ21aを復号する復号手段23と、復号手段23が復号したデータに含まれる命令に従って、復号したデータを処理する処理手段2と、暗号化方式決定手段12及び復号方式決定手段22で取り扱う暗号化方式と復号方式とを対応づける暗号化／復号方式管理手段3と、を有することを特徴とする情報処理装置が提供される。

【0041】この情報処理装置によれば、暗号化対象データ1は任意の暗号化方式により暗号化され暗号データ11aとなる。さらに、暗号化方式を示す暗号化方式識別データ12aが暗号データ11a内に配置された暗号データ13aが生成される。暗号データ13aは、記憶手段30に格納される。そして、暗号データ13aのデータ処理が必要になると、分離手段21により、暗号データ13aが復号対象データ21aと復号方式識別データ21bとに分離される。そして、復号方式決定手段22が、復号方式識別データ21bから復号方式を決定し、その復号方式により復号手段23が、復号対象データ21aを復号する。復号手段23により復号されたデータ2aは、暗号化対象データ1と同一のデータとなる。データ2aは、自己に含まれた命令に基づき、処理手段2によって処理される。暗号化方式決定手段12及び復号方式決定手段22で取り扱う暗号鍵や復号鍵及び暗号化アルゴリズムや復号アルゴリズムは、暗号化／復号方式管理手段3で管理されており、識別データに対応した暗号鍵や復号鍵及び暗号化アルゴリズムや復号アルゴリズムが暗号化／復号方式管理手段3から供給される。

【0042】このようにして、暗号データ内に識別データを含ませることによりコンピュータのメモリの管理方法に依存せずに、復号の際の復号アルゴリズムと復号鍵とを特定することができる。

【0043】

【発明の実施の形態】以下、本発明の実施の形態を図面

に基づいて説明する。図1は本発明の情報処理装置の原理構成を示す図である。本発明の情報処理装置は、入力された暗号化対象データ1を暗号化する暗号化装置10、処理を行うべきデータを復号して出力する復号装置20、暗号化装置10で暗号化された暗号化データ13aを格納しておく記憶手段30、復号手段23が復号したデータに含まれる命令に従って、復号したデータを処理する処理手段2、及び暗号化方式決定手段12及び復号方式決定手段22で取り扱う暗号化方式と復号方式とを対応づける暗号化／復号方式管理手段3から構成される。

【0044】暗号化装置10には、暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段12と、暗号化方式決定手段12により決定された暗号化方式を用いて暗号化対象データ1を暗号化し、暗号化データ11aを生成する暗号化手段11と、暗号化データ11aの暗号化に用いられた暗号化方式を示す暗号化方式識別データ12aを、暗号化データ内の所定の位置に配置する配置手段13とが設けられている。

【0045】復号装置20には、記憶手段30に格納された暗号化データ13aを、復号対象データ21aと復号方式識別データ21bとに分離する分離手段21と、分離手段21により分離された復号方式識別データ21bに応じて、復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段22と、復号方式決定手段22で決定された復号方式を用いて、復号対象データ21aを復号する復号手段23とが設けられている。

【0046】この情報処理装置によれば、暗号化装置10に暗号化対象データ1が入力されると、暗号化方式決定手段12は暗号化方式識別データ12aを定め、その暗号化方式識別データ12aに応じた暗号鍵及び暗号化アルゴリズムが、暗号化／復号方式管理手段3から暗号化方式決定手段12に供給される。暗号化方式決定手段12は、暗号化対象データ1の暗号化方式を、暗号化／復号方式管理手段3から供給された暗号化方式に決定する。そして、暗号化対象データ1は、暗号化方式決定手段12が決定した暗号化方式で、暗号化手段11により暗号化され暗号化データ11aとなる。さらに、配置手段13により、暗号化方式を示す識別データ12aが暗号化データ11a内に配置され暗号化データ13aとなる。この暗号化データ13aは、記憶手段30に格納される。これで、暗号化の処理は終了する。

【0047】暗号化データ13aのデータ処理を行う要求が発生すると、復号装置20内の分離手段21が、記憶手段30に格納されている暗号化データ13aを復号対象データ21aと復号方式識別データ21bとに分離する。すると、復号方式決定手段22は、暗号化／復号方式管理手段3から復号方式識別データ21bに応じた

復号鍵及び復号アルゴリズムの供給を受ける。そして、復号方式決定手段22は、復号対象データ21aの復号方式を、暗号化／復号方式管理手段3から供給された復号方式に決定する。復号対象データ21aは、復号方式決定手段22で決定された復号方式で、復号手段23により復号される。復号されたデータ2aは、暗号化対象データ1と同じ内容のデータに戻っている。処理手段2は、復号されたデータ2aに含まれる命令に従って処理を行う。

【0048】これにより、暗号化方式は任意に定めることができるため、暗号化アルゴリズムと暗号鍵との組み合わせを複数用意し、暗号化対象データごとに異なる暗号化方式とすることができる。そのため、少ない計算量の暗号化アルゴリズムであっても暗号化強度の高い暗号化データを得ることができる。さらに、暗号化データ内に識別データを含ませることにより、復号の際には、コンピュータのメモリの管理方法に依存せずに復号方式を特定することができる。しかも、暗号化方式と復号方式とは、暗号化／復号方式管理手段3によって対応関係が管理されているため、もし暗号化データ内の識別データの位置が解読されたとしても、復号アルゴリズムや復号鍵が露呈することはなく、その暗号化データの復号方式を解読することはできない。

【0049】図2は本発明を実施するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。ソフトウェアの保護機能付き情報処理装置は、プログラムに従ってデータの処理を行うMPU (Micro Processing Unit) 111と、MPU 111で取り扱われるデータの暗号化及び復号を行う暗号化／復号装置112と、暗号化／復号装置112で用いる暗号鍵及び復号鍵を格納する鍵テーブル113と、MPU 111によって処理されるデータを転送するためのシステムバス113と、暗号化／復号装置112で暗号化されたデータを格納するメインメモリ121と、I/Oインターフェース122と、I/Oインターフェース122を介して接続される補助メモリ123から構成されている。

【0050】ここでは示していないがMPU 111は内部にキャッシュメモリを含んでいる場合もある。また、メインメモリ121は主にRAM (Random Access Memory) 等で構成される。補助メモリ123はハードディスク、フロッピーディスク、CD-ROM等で構成される。暗号化／復号装置112は、暗号化及び復号のアルゴリズムは特定されており、暗号鍵と復号鍵が決まることにより、データの暗号化及び暗号化データの復号を実行することができる。

【0051】図2に従ってソフトウェアの保護機能付き情報処理装置の動作を説明する。保護を受けるデータは、暗号化／復号装置112で暗号化された後に、メインメモリ121または補助メモリ123に格納される。この時、暗号化／復号装置112で用いる暗号化には複

数の暗号鍵が用意され、暗号鍵は暗号化されるデータの特定の数ビットを参照することにより鍵テーブル113から選択される。どのビットをどのように参照するか、その方法はソフトウェアの保護機能付き情報処理装置の各々に関して決定される。暗号化されたデータがMPU111で処理される時は、まず暗号化／復号装置112へ読み込まれ、MPU111が処理を行えるように復号される。復号する時に用いられる復号鍵は、暗号化されているデータの特定の数ビットを参照することで、鍵テーブル113から選択される。この時の参照する数ビットを選ぶ方法は、前述の暗号鍵の選択の際に使用した方法との関係が一意であるように決定されている。MPU111で処理されたデータが再びメインメモリ121または補助メモリ123に格納される時は、暗号化／復号装置112により再び暗号化される。以下、暗号化／復号装置112で行われる暗号化の詳細な説明を図3及び図4を用いて、また復号の詳細な説明を図5及び図6を用いて行う。

【0052】図3は、図2に示される暗号化／復号装置112で用いられる暗号化方法のフローチャートを示す。このフローチャートの説明を行う。

【S1】暗号化されるべきデータを暗号化／復号装置112へ読み込む（ステップ1）。

【S2】暗号化／復号装置112において、読み込んだデータから特定の数ビットを抜き出す（ステップ2）。

【S3】ステップ2において抜き出した数ビットに対応する暗号鍵を、鍵テーブル113より選択する（ステップ3）。

【S4】ステップ3において選択した暗号鍵を用いて、暗号化されるべきデータの、抜き出した数ビット以外の部分を暗号化する（ステップ4）。

【S5】暗号化したデータに、ステップ2において抜き出した数ビットを埋め込む（ステップ5）。

【0053】以上の各ステップにおいて、暗号化されるデータの状態がどのように変化するかを、図4の状態遷移図に従って説明する。なお、鍵テーブル113に格納される内容は、暗号化／復号方式ごと異なる。そこで、以後の説明において、鍵テーブル113の内容に言及する場合には、鍵テーブルには暗号化／復号方式ごとに個別の番号を付すこととするが、ハードウェアとしては図2に示す鍵テーブル113を指している。

【0054】(A)は、ステップ1の状態を示す図である。暗号化すべきデータ31が読み込まれる。暗号化される前のデータ31は32ビットからなり、MPU111で直接処理を行うことのできる状態にある。

【0055】(B)は、ステップ2の状態を示す図である。暗号化される前のデータ31から、特定の数ビットを抜き出す。例では7、11、15及び23ビット目の4ビットのデータを抜き出している。従って、28ビットのデータ32が残ることとなる。抜き出したビット

は、所定の配列に並べられビット情報33となる。このビット情報33は、図1に示す暗号化方式識別データ12aに対応する。(C)は、ステップ3の状態を示す図である。4ビットのビット情報33に対応する暗号鍵を、予め用意された鍵テーブル40から選択する。鍵テーブル40は図2における鍵テーブル113にあたり、抜き出したビットによるビット情報40aに対応する鍵40bが一意に選択できるようになっている。例では抜き出すビット数が4ビットであることから鍵も4ビットで分類されており、16個のビット情報「0000」, 「0001」, 「0010」・・・のそれぞれに対応する16個の鍵41, 42, 43・・・が存在する。この例では、抜き出したビットによるビット情報33の値が「0010」であるため、鍵43が暗号鍵として選択されている。

【0056】(D)は、ステップ4の状態を示す図である。選択された鍵43を暗号鍵に用いて、抜き出した4ビットのビット情報33以外の28ビットのデータ32を暗号化し、28ビットの暗号化データ34を生成する。

【0057】(E)は、ステップ5の状態を示す図である。(B)において抜き出した4ビットのビット情報33を、28ビットの暗号化データ34に埋め込み、32ビットの暗号化データ35としてメインメモリ121に格納する。

【0058】抜き出した4ビットのビット情報33を埋め込む方法は、復号の際にビット情報33を分離するための方法とセットで決定されている。この2つの方法が一意に決定できるのであれば、埋め込む位置を最初に抜き出したビット位置と同じにする必要はない。また、最後にスクランブル等を行い、第三者に暗号鍵の選択に用いたビットの位置を容易に見つけられないようにすることも可能である。なお、最後にスクランブルを行う場合には、ステップ4で行う暗号化はスクランブル以外の方法であることが望ましい。更に、抜き出した4ビットのビット情報33を暗号化した28ビットのデータ34に埋め込む際、XOR等の暗号化方法で暗号化して埋めこんでもよい。

【0059】図5には、図2に示される暗号化／復号装置112で用いられる復号方法のフローチャートを示す。このフローチャートの説明を行う。

【S11】暗号化されているデータを暗号化／復号装置112へ読み込む（ステップ11）。

【S12】暗号化／復号装置112において、読み込んだデータから鍵の選択に用いた数ビットを抜き出す（ステップ12）。

【S13】ステップ12において抜き出した数ビットに対応する復号鍵を、鍵テーブル113より選択する（ステップ13）。

【S14】ステップ13において選択した復号鍵を用い

て、復号されるべきデータの、抜き出した数ビット以外の部分を復号する（ステップ14）。

【S15】復号したデータに、ステップ12において抜き出した数ビットを埋め込む（ステップ15）。

【0060】復号されるデータの状態がどのように変化するかを、図6の状態遷移図に従って説明する。32ビットのデータを復号する場合を考える。但しこの32ビットのデータは、図3及び図4に示した暗号化方法に従って暗号化された後、メインメモリ121に格納されていたものとする。なお、この例は暗号鍵と同じ鍵を復号鍵とする場合である。

【0061】(A)は、ステップ11の状態を示す図である。暗号化データ35を記憶装置から読み込む。暗号化データ35は32ビットからなり、MPU111で直接処理を行うことのできない状態にある。

【0062】(B)は、ステップ12の状態を示す図である。暗号化データ35から、特定の数ビットを抜き出し、ビット情報33を得る。例では6、13、27及び30ビット目の4ビットを抜き出している。この4ビットのデータを抜き出す位置は、暗号化の際に、ビット情報33の各ビットを埋め込んだ位置である。この結果、28ビットの暗号化データ34が残ることとなる。

【0063】(C)は、ステップ13の状態を示す図である。抜き出した4ビットのビット情報33に対応する鍵43を、予め用意された鍵テーブル40から選択する。ビット情報33の値は「0010」であるため、鍵テーブル40を用いて、暗号化の際の鍵43と同一の鍵43を選択することができる。この選択された鍵43が復号鍵となる。

【0064】(D)は、ステップ14の状態を示す図である。選択した鍵43を復号鍵として、抜き出した4ビットのビット情報33以外の28ビットの暗号化データ34を復号し、28ビットのデータ32を生成する。

【0065】(E)は、ステップ15の状態を示す図である。(B)において抜き出した4ビットのビット情報33を、28ビットのデータ32に埋め込み、32ビットのデータ31を得る。埋め込む位置は、暗号化の際に4ビットのデータを抜き出した位置と同じ位置である。この結果、暗号化する前のデータと同一のデータ31が得られる。

【0066】以上のような方法により、復号鍵の抽出に用いるデータが復号の対象となる暗号化されたデータの一部で構成される。そのため、余分な情報をデータに付加する必要がなく、メモリ空間を有効に使用できる。上記の例では具体的なビット数を示して説明を行ったが、これは説明を解りやすくするためであり、ビット数はソフトウェアの保護機能付き情報処理装置の各々で任意に選ぶことができる。従ってある単位、例えばバスで取り扱うビット単位（8ビット、16ビット、32ビット、64ビット、128ビット等）や仮想記憶で用いられる

ページ単位、キャッシュメモリのデータを交換するビット単位等に関連させて暗号化のブロックを選択することで効率的な暗号化及び復号を行うことができる（このことは以下の説明においても同様である）。

【0067】上記の例では、暗号化の鍵と復号の鍵とを選択する際に、同じ鍵テーブルを用いているため、暗号鍵と復号鍵が同一となっているが、暗号化の鍵テーブルと復号の鍵テーブルとを個別に設けることにより、暗号鍵と復号鍵とを個別のものにすることができる。これにより、暗号化の際に用いた暗号鍵と異なる復号鍵により復号するような暗号化／復号アルゴリズムを利用することもできる。

【0068】また、上記の例では抜き出した数ビットから暗号鍵を選択する時に鍵テーブルを用いたが、抜き出した数ビットをある特定の関数に入力し、その出力値を暗号鍵として用いてもよく、そのようにすれば鍵テーブルを持つ必要がなくなる。勿論抜き出した特定の数ビットそのものを暗号鍵としてもよい。

【0069】以上のような方法により、メインメモリ121または補助メモリ123に格納されたデータの内容を秘密にすることができる。また、暗号鍵及び復号鍵の選択がデータだけに依存しており、保護の対象であるデータの一部あるいは全部から暗号鍵を導出することができるため、特にアドレスに依存せずに、複数の暗号鍵でデータを暗号化することができる。その為、OSによる複雑なアドレス管理が行われている場合でも、OSに依存することなく複数の暗号鍵を管理することができる。つまり、OSを改ざんすることにより秘匿データを盗用するという攻撃に対して、有効な防御を実現することができる。

【0070】また、暗号化に複数の暗号鍵を使用しているので、計算量の少ない暗号化方法（例えばXORなど）を用いても十分な暗号強度を得ることができ、暗号化及び復号のプロセスがデータの処理速度に及ぼす影響を少なくすることができる。従って、メモリ中のデータを逐次復号しながらプログラムを実行する場合でも十分な実行速度と暗号強度を実現することができる。これにより、常にメインメモリ中に常駐するようなOS自身を防御することも可能である。

【0071】上記の例は、暗号化及び復号のアルゴリズムが一定であり、データごとに異なる暗号鍵と復号鍵とを使用した場合であるが、データごとに異なる暗号化及び復号のアルゴリズムを使用することもできる。図7は複数の暗号化及び復号のアルゴリズムを使用するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。このソフトウェアの保護機能付き情報処理装置は、プログラムに従ってデータの処理を行うMPU（Micro Processing Unit）211と、MPU211で取り扱われるデータの暗号化及び復号を行う暗号化／復号装置212と、暗号化／復号装置212で用いる

暗号化／復号のアルゴリズム及び暗号／復号鍵を格納する暗号化／復号アルゴリズム&鍵テーブル214と、MPU211によって処理されるデータを転送するためのシステムバス231と、暗号化／復号装置212で暗号化されたデータを格納するメインメモリ221と、I/Oインターフェース222と、I/Oインターフェース222を介して接続される補助メモリ223から構成されている。

【0072】ここでは示していないがMPU211は内部にキャッシュメモリを含んでいる場合もある。また、メインメモリ221は主にRAM等で構成される。補助メモリ223はハードディスク、フロッピーディスク、CD-ROM等で構成される。暗号化／復号アルゴリズム&鍵テーブル214は、XORやシフト等の複数種の暗号化アルゴリズム214aと、各暗号化アルゴリズムに一意に対応する同数の復号アルゴリズム214bと、各暗号化アルゴリズムに一意に対応する同数の暗号鍵214c、及び各復号アルゴリズム214bに一意に対応する同数の復号鍵214dを持つ。ここで、対応関係にある暗号化アルゴリズムと復号アルゴリズムとは、同じ方式のアルゴリズムである。

【0073】この装置の動作は図2に示したソフトウェア保護機能付き情報処理装置とほぼ同様であるが、この例では暗号化される前のデータから抜き出す特定の数ビットを用いて、暗号化アルゴリズムの選択を行う。1つの暗号化アルゴリズムには、暗号鍵と、復号アルゴリズムと、復号鍵がそれぞれ1つずつ対応し、暗号化／復号アルゴリズム&鍵テーブル214に記憶されている。復号する場合は抜き出した特定の数ビットから復号アルゴリズム及び復号鍵を抽出して、データの復号を行う。

【0074】このような方法で複数の暗号化／復号のアルゴリズムを用いてデータを暗号化することができ、更に暗号強度を高くすることができる。以上の2つの例では、いずれも暗号化の対象となるデータから抜き出されたビットを基に暗号鍵や暗号アルゴリズムを特定しているが、暗号鍵と暗号化対象データとの関連性は必ずしも必要ではない。そのため、任意の鍵を適当に選択して暗号鍵とすることもできる。なお、任意の鍵を適当に選択して暗号鍵とする場合の基本的なハードウェア構成については図2に示したソフトウェア保護機能付き情報処理装置と同じであり、暗号化／復号装置112の機能のみが異なる。そこで、適当に選択した鍵を暗号鍵とする場合の暗号化／復号装置の処理機能のみを、以下に説明する。

【0075】図8は適当に選択した鍵を暗号鍵とする場合のフローチャートである。

【S21】暗号化されるべきデータを暗号化／復号装置へ読み込む（ステップ21）。

【S22】暗号鍵を、鍵テーブルより任意に選択する（ステップ22）。

【S23】ステップ22において選択した暗号鍵を用いて、暗号化されるべきデータ全てを暗号化する（ステップ23）。

【S24】暗号化されたデータに、ステップ22において選択した暗号鍵のビット情報を埋め込む（ステップ24）。

【0076】次に、これらの各ステップにより、暗号化されるデータの状態がどのように変化するかを、図9の状態遷移図に従って説明する。ここでは、32ビットのデータを暗号化する場合を考える。なお、図9における鍵テーブル60は、図1における鍵テーブル113に相当する。鍵の長さとしては、例えば暗号化対象データと同じビット数、すなわち32ビットを採用する。このように鍵のビット数も長くすること（できれば、暗号化対象データ長と同じビット数）によって、単に鍵を入力データから抽出した場合に比べ暗号化強度の向上が図れる。

【0077】(A)は、ステップ21の状態を示す図である。暗号化される前のデータ51は32ビットからなり、MPUで直接処理を行うことのできる状態にある。

(B)は、ステップ22の状態を示す図である。鍵テーブル60から任意に暗号鍵を選択し、対応するビット情報を調査する。鍵テーブル60内の鍵60bには、全て一意に定められた分類のためのビット情報60aが対応しており、図では4ビットの分類がされているので、合計16個の鍵61、62、63、・・・にビット情報「0000」、「0001」、「0010」・・・が対応付けられている。この例では、鍵63が暗号鍵として選択されたものとする。鍵63に対応するビット情報の値は「0010」である。

【0078】(C)は、ステップ23の状態を示す図である。選択した鍵63を暗号鍵に用いて、32ビットのデータ51を全て暗号化し、32ビットの暗号化データ52を生成する。

【0079】(D)は、ステップ24の状態を示す図である。(B)において調査したビット情報53を、32ビットの暗号化データ52に埋め込み、36ビットの暗号化データ54として記憶装置に格納する。

【0080】調査した情報ビット53を埋め込む方法は、ソフトウェアの保護機能付き情報処理装置の各々によって、任意に決定される。暗号化データ54を復号する場合は上記と逆のステップを行い、データ51を得る。

【0081】以上のような方法により、暗号鍵の選択をデータに依存せずに行うことができる。また復号鍵を選択する場合に鍵テーブルを用いず、ある特定の関数に抜き出した4ビットを入力すると復号鍵が得られるようにしてもよい。

【0082】次に、暗号化データに暗号鍵の情報を埋め込むのではなく、ハッシュ関数を用いて暗号化データと

暗号鍵とを対応付けるソフトウェアの保護機能付き情報処理装置について説明する。

【0083】図10はハッシュ関数を用いて暗号化データと暗号鍵とを対応付ける場合のフローチャートである。これは、図2に示すソフトウェアの保護機能付き情報処理装置内部の、暗号化／復号装置112で用いる暗号化方法を変更したものの1つである。暗号化／復号装置以外の機能については図2に示すソフトウェアの保護機能付き情報処理装置と同じであるため、この例では、暗号化／復号装置の処理機能のみを説明する。

【S31】暗号化されるべきデータを暗号化／復号装置112へ読み込む（ステップ31）。

【S32】暗号鍵を、鍵テーブル113より任意に選択する（ステップ32）。

【S33】ステップ32において選択した暗号鍵を用いて、暗号化されるべきデータ全てを暗号化する（ステップ33）。

【S34】暗号化したデータのハッシュ値を計算する（ステップ34）。

【S35】ステップ34において計算したハッシュ値と、暗号鍵をセットにしてハッシュテーブルに登録する（ステップ35）。

【0084】暗号化されるデータの状態がどのように変化するかを、図11の状態遷移図に従って説明する。この例では、32ビットのデータを暗号化する場合を考える。なお、図11における鍵テーブル80は、図2における鍵テーブル113に相当する。

【0085】(A)は、ステップ31の状態を示す図である。暗号化される前のデータ71は32ビットからなり、MPUで直接処理を行うことのできる状態にある。

(B)は、ステップ32の状態を示す図である。鍵テーブル80内の鍵80bには、全て一意に定められた分類のためのビット情報80aが対応している。図では4ビットの分類がされているので、合計16個の鍵81、82、83、・・・にビット情報「0000」、「0001」、「0010」・・・が対応付けられている。この例では、鍵83が暗号鍵として選択されたものとする。鍵83に対応するビット情報の値は「0010」である。

【0086】(C)は、ステップ33の状態を示す図である。選択した鍵83を暗号鍵に用いて、32ビットのデータ71を全て暗号化し、32ビットの暗号化データ72を生成する。

【0087】(D)は、ステップ34の状態を示す図である。32ビットの暗号化データ72をハッシュ関数84に入力して、ハッシュ値73を得る。(E)は、ステップ35の状態を示す図である。ハッシュ値73と、暗号化に使用した鍵83をセットにして、ハッシュテーブル90に登録する。ハッシュテーブル90はハッシュ値90aと鍵90bとが各々一意に対応している。図で

は、ハッシュ値「01010001」、「00010100」、「10010111」・・・に対応して鍵91、92、93・・・が登録されている。32ビットの暗号化データ72は記憶装置に格納される。

【0088】暗号化されたデータを復号する場合には、暗号化されたデータのハッシュ値を求めハッシュテーブルより鍵を抽出し、その鍵を復号鍵として復号を行う。以上のような手段により、暗号化されたデータのハッシュ値からハッシュテーブルを基に復号鍵を抽出できるので、OSによる複雑なアドレス管理が行われている場合でもOSに依存することなく複数の暗号鍵を管理することができる。また、ハッシュ関数を用いることで、暗号化されるデータの膨大なデータ空間（この例では232ビット）をハッシュ値のデータ空間（この例では28ビット）に圧縮することができるので、鍵の管理に用いるメモリ空間を小さくすることができる。

【0089】なお、異なる2つのデータが、それぞれ異なる暗号鍵によって暗号化されたにも拘わらず同じハッシュ値を持つようになってしまった場合、1つのハッシュ値に対して暗号鍵が2つ存在することになり、どちらの暗号鍵を用いて暗号化したのか判らなくなることが考えられる。このような場合は、暗号化したデータのハッシュ値が、既に登録されているものと同じになった時点で、もう一度更に異なる暗号鍵で暗号化する等の処置をとることで問題を解決する。なお、この場合には、暗号化されたデータのハッシュ値が他のハッシュ値と同じでないことを確認するまで、暗号化前のデータをバッファ等に保持しておく必要がある。

【0090】以上の例では、情報処理装置の内部で暗号化したデータを復号して実行する場合を想定しているが、これだけでは、この情報処理装置で使用するためのソフトウェアを、他の装置で開発することが難しくなってしまう。そこで、他の装置から提供されるデータを復号するための別の復号装置を新たに設けることにより、この問題に対処することができる。以下にその例を説明する。

【0091】図12は他の装置から提供される暗号化データを復号できるソフトウェアの保護機能付き情報処理装置を示すブロック図である。このソフトウェアの保護機能付き情報処理装置は、データの処理を行うMPU

(Micro Processing Unit) 311と、暗号化されたデータの復号を行う復号装置312と、復号されたデータをすぐに暗号化する暗号化装置313と、暗号化装置313で暗号化されたデータを記憶するメインメモリ321と、暗号化装置313で暗号化され、メインメモリ321に記憶されているデータの復号を行う復号装置314と、システムバス331と、I/Oインターフェース(I/O) 322と、補助メモリ323及びネットワーク325から構成されている。

【0092】さらに、MPU 311、復号装置312、

暗号化装置 313 及び復号装置 314 は、外部からの観測またはプログラム及びデータの改ざんを防止する安全保護容器 310 内に格納されている。安全保護容器としては特開昭 63-124153 号公報「記憶情報保護装置」に示されたようなものを用いることができる。この安全保護容器は、複雑な経路をたどる導体路が表面に形成された包囲体で秘密情報を取り扱う回路カードを囲み、内部の秘密情報を不正に解析しようとして包囲体を破壊した場合に導体路の切断や短絡が生じ、それをトリガーとして秘密情報を消去するという構造になっている。

【0093】以上の構成において、まずデータは暗号化された状態で、ネットワーク 325 や CD-ROM 等によってソフトウェア提供者からユーザに提供される。この時用いられる暗号化方式は汎用的で暗号強度の高いものである。例えば、ソフトウェア提供者は前記暗号化方式として DES (Data Encryption Standard) 等を用いてユーザに提供するデータを暗号化する。そして暗号鍵は例えば RSA (Rivest Shamir Adleman : Ronald Rivest, Adi Shamir, Leonard Adleman) の 3 氏が考案したアルゴリズム) 暗号によってソフトウェアの保護機能付き情報処理装置の公開鍵で暗号化され、暗号化されたデータとペアにしてユーザに提供される。ユーザは、DES を用いて暗号化されたデータを I/O 322 を介して復号装置 312 に送る。

【0094】復号装置 312 で復号されたデータは、直接暗号化装置 313 に送られソフトウェアの保護機能付き情報処理装置各々に固有の非公開の暗号化アルゴリズム及び暗号鍵で暗号化される。この際の暗号化アルゴリズム及び暗号鍵を特定するための識別情報は、暗号化されたデータ内の所定の位置に埋め込まれるか、あるいは、暗号化されたデータのハッシュ値に対応付けて管理される。暗号化装置 313 で暗号化されたデータはメインメモリ 321 に格納される。

【0095】MPU 311 はメインメモリ 321 に格納されている暗号化されたデータを復号装置 314 で復号して受け取り、実行する。復号装置 314 が復号を行う際の復号鍵及び復号アルゴリズムは、暗号化データに埋め込まれた識別情報を解析するか、あるいは暗号化データのハッシュ値から求めることができる。MPU 311 が処理を終了し出力するデータの中で暗号化が必要なものは、暗号装置 313 で暗号化してからメインメモリ 321 に格納される。

【0096】以上のように、公開された暗号方式と暗号鍵を用い暗号化されたデータを、ソフトウェアの保護機能付き情報処理装置内に取り込んで復号装置 312 で復号できるので、ソフトウェアの供者は暗号化装置 313 及び復号装置 314 で使用する暗号化／復号方式または暗号／復号鍵を知る必要はなく、ただ MPU 311 用にソフトウェアの開発すればよい。つまり、ソフトウェア

の保護機能付き情報処理装置内の暗号化／復号方式または暗号／復号鍵を知りえない第三者が、ソフトウェアの保護機能付き情報処理装置に守られるソフトウェアの自由に開発できる。また、復号されたデータは直接暗号化されるので、ユーザが復号されたデータにアクセスすることはできない。

【0097】暗号化装置 313 及び復号装置 314 で用いられる暗号化方法及び復号方法に、前の例で示したように、アルゴリズムと鍵とを特定する識別情報を暗号化データに埋め込んだり、あるいはハッシュ値と識別情報を対応付ける方法を用いることにより、暗号化に複数の暗号鍵を使用できる。これにより、計算量の少ない暗号化アルゴリズムを利用しても十分な暗号強度を得ることができる。その結果、暗号化及び復号のプロセスがデータの処理速度に及ぼす影響を小さくすることができ、メモリ中のデータを逐次復号しながらプログラムを実行する場合でも、十分な実行速度と暗号強度を実現できる。

【0098】また、暗号化装置 313 及び復号装置 314 で用いられる暗号化方法及び復号方法は、他の情報処理装置と共有する必要がないので、暗号化及び復号のアルゴリズムや暗号鍵及び復号鍵を、1つの情報処理装置内だけで独自に設定または更新することが可能である。ある条件 (例えば電源オン／オフや 1 日ごと) で暗号化及び復号のアルゴリズムや暗号鍵及び復号鍵を更新するようにすれば、さらに暗号強度を高めることができる。電源オン／オフ時に暗号鍵及び復号鍵を更新するには、図 2 に示した鍵テーブル内の鍵の値を電源オン時に変更すればよい。

【0099】また、MPU 311、復号装置 312、暗号化装置 313 及び復号装置 314 が安全保護容器 310 内に格納されているため、内部の秘密情報を不正に解析しようとする、安全保護容器 310 の包囲体が破壊され、秘密情報が消去される。その結果、暗号鍵、復号鍵及び暗号化されていないデータ等を取り扱う MPU、暗号化装置及び復号装置を安全保護容器内に格納すれば、不正を行おうとする者は暗号を解読する手掛かりをほとんど失うことになり、プログラム及びデータの秘匿性が、さらに高められる。

【0100】ところで、図 12 で示した例は他の装置で開発されたソフトウェアを受け取るための情報処理装置であるが、逆に、自己の内部で開発したソフトウェアを他の装置へ暗号化して送信する場合には、別の暗号化装置を新たに設ける。この暗号化装置では、DES 等の暗号強度の高い暗号アルゴリズムで暗号化を行う。これにより、開発途中のソフトウェアは、計算量の少ないアルゴリズムと複数の鍵を組み合わせることにより暗号強度を高め、ソフトウェアを他の装置へ送信する際には、暗号強度の高いアルゴリズムを用いて暗号強度を高めることができる。

【0101】なお、以上の本発明の説明では MPU やメ

インメモリ等の現在コンピュータシステムで使われている用語を用いたが、これらの用語は本発明をなんら限定するものではなく同等の機能を有するものであればよい。また、計算量の少ない暗号化及び復号アルゴリズムとして、XOR、シフト及びスクランブル等を例にして述べてきたが、これらはコンピュータの処理能力が向上してくれば、さらに複雑な暗号化及び復号アルゴリズムと置き換えることが可能である。

【0102】図13は本発明の情報処理装置の他の実施形態を示す図である。図13において、340はネットワーク等から暗号化された情報を取り込み記憶する記憶装置を表す。350は記憶手段340に格納されている暗号化された情報を復号し、処理装置360が処理できるように復号する復号装置を表す。復号装置350には分離手段351、復号方式決定手段352、復号手段353、復号方式管理手段354、及び再配置手段355が含まれており、これらにより記憶装置340内に格納された暗号化されたデータ341の復号を行う。処理装置360は復号装置350により復号されたデータに基づいて処理を行う。図13の装置の動作を以下に説明する。

【0103】記憶装置340は、ネットワークやCD-ROM等から暗号化されたデータを取り込み格納する。記憶装置340に格納されたデータ341は、復号装置350内の分離手段351に読み込まれ復号対象データ351aと認識データ351bとに分離される。そして、復号対象データ351aは復号手段353に読み込まれ、認識データ351bは復号方式決定手段352に読み込まれる。復号方式決定手段352は認識データ351bに対応した復号方式を復号方式管理手段354から選択し、復号アルゴリズム又は復号鍵を復号手段353に与える。復号手段353は与えられた復号アルゴリズム又は復号鍵を用いて復号対象データ351aを復号する。復号手段353で復号されたデータと認識データ351bは再配置手段355により結合され、処理装置360で取り扱うことのできるデータ361となり、処理装置360により処理される。

【0104】このように、本発明の実施形態には復号装置のみを有する構成も考えられ、暗号化された情報は、予め復号方式管理手段354に保持されている復号方法と対応した暗号化方法を用いて暗号化されてネットワークやCD-ROM等で提供される。この装置構成が適用される領域としては、与えられた情報を変更する必要のない家庭用ゲーム機器や電子出版物等が挙げられる。また、これらの装置で取り扱う情報を暗号化する装置は、暗号化装置のみを有する構成となる。

【0105】また、暗号化すべきデータから抜き出すべき数ビットとして、パリティビットを用いることもできる。その例を以下に示す。この場合のハードウェア構成は、図2に示した制御装置と同様の構成であるため、図

2の構成を用いて説明する。

【0106】図14は、パリティビットにより鍵を特定する暗号化方法のフローチャートである。以下に、このフローチャートの説明を行う。ここでは、暗号化されていない32ビットデータを4組で、暗号化の1単位とした場合を考える。

【S41】暗号化／復号装置112は、暗号化されていない4組の32ビットデータを読み込む（ステップ41）。

【S42】暗号化／復号装置112において、32ビットデータごとのパリティビットを算出し、暗号鍵の選択に用いる4ビットを得る（ステップ42）。

【S43】ステップ42において算出した4ビットに対応する暗号鍵を、予め用意している鍵テーブル113から選択する。それぞれの暗号鍵は4ビットで分類されており、この場合、合計16個の暗号化鍵が存在する（ステップ43）。

【S44】ステップ43において選択した暗号鍵を用いて、入力データを暗号化する（ステップ44）。この際、パリティビットの値が変化しないような暗号化方式を用いる。例えば、スクランブルや置換等である。

【S45】算出した4ビットをパリティビットとして暗号化したデータに付加してメインメモリ121又は補助メモリ123に格納する（ステップ45）。

【0107】以上の各ステップにおいて、暗号化されるデータがどのように変化するかを、図15の状態遷移図に従って説明する。この図において、鍵テーブル410は図2の鍵テーブル113の内容を示すものである。

【0108】(A)は、ステップ41の状態を示す図である。暗号化すべきデータ401が読み込まれる。暗号化される前のデータ401は、32ビットのデータが4つで1単位である。

【0109】(B)は、ステップ42の状態を示す図である。暗号化される前のデータ401から、32ビットのデータごとのパリティビットを求める。求められたパリティビットが所定の配列に並べられ、4ビットのビット情報402となる。

【0110】(C)は、ステップ43の状態を示す図である。4ビットのビット情報402に対応する暗号鍵を、予め用意された鍵テーブル410から選択する。鍵テーブル410は図2における鍵テーブル113にあたり、ステップ42で抜き出したビット情報402に対応する鍵413が一意に選択できる。この例では抜き出すビット数が4ビットであることから鍵も4ビットで分類されており、16個のビット情報「0000」、「0001」、「0010」・・・のそれぞれに対応する16個の鍵411、412、413・・・が存在する。この図では、ビット情報402の値「0010」に対応する鍵413が暗号鍵として選択される。

【0111】(D)は、ステップ44の状態を示す図で

ある。選択された鍵413を暗号鍵に用いて、32ビット×4のデータ401を暗号化し、暗号化データ403を生成する。なお、この際の暗号化方式は、パリティビットの値が変化しないような暗号化方式である。

【0112】(E)は、ステップ45の状態を示す図である。(B)において算出した4ビットのビット情報402を、暗号化データ403のパリティビットとして付加し、パリティビット付きの暗号化データ404がメインメモリ121に格納される。

【0113】図16はパリティビットにより鍵を特定する復号方法のフローチャートである。

【S51】1組として暗号化されているデータ404を暗号化／復号装置112へ読み込む(ステップ51)。

【S52】暗号化／復号装置112において、読み込んだデータからパリティビットを抜き出し、復号鍵の選択に用いる4ビットのビット情報402を得る(ステップ52)。

【S53】ステップ52において抜き出したビット情報402に対応する復号鍵413を、鍵テーブル410より選択する(ステップ53)。

【S54】ステップ53において選択した復号鍵413を用いて、復号されるべきデータ404の、パリティビット以外の部分を復号する(ステップ54)。

【0114】図17は図16の各ステップの状態遷移図である。なお、この例は暗号鍵と同じ鍵を復号鍵とする場合である。(A)は、ステップ51の状態を示す図である。暗号化データ404を記憶装置から読み込む。暗号化データ404は32ビット×4のデータとパリティビットからなり、MPU111で直接処理を行うことができない状態にある。

【0115】(B)は、ステップ52の状態を示す図である。暗号化データ404から、パリティビットを抜き出し、ビット情報402を得る。この結果、暗号化データ403が残ることとなる。

【0116】(C)は、ステップ53の状態を示す図である。抜き出した4ビットのビット情報402に対応する鍵413を、予め用意された鍵テーブル410から選択する。ビット情報402の値は「0010」であるため、鍵テーブル410を用いて、暗号化の際の鍵と同一の鍵413を選択することができる。

【0117】(D)は、ステップ54の状態を示す図である。選択した鍵413を復号鍵として、抜き出した4ビットのビット情報402以外の暗号化データ403を復号し、32ビット×4のデータ401を生成する。

【0118】なお、以上の説明で具体的なビット数が示したが、これは説明を分かりやすくするためであり、ビット数を任意に選ぶことができることは、図3～図6で示した暗号化／復号方法と同様である。即ち、例えばバスで取り扱うビット単位(8ビット、16ビット、32ビット、64ビット、128ビット等)や仮想記憶で用

いられるページ単位やキャッシュメモリのライン(ブロック)単位等に関連させて暗号化のブロックを選択することで効率的な暗号化及び復号を行うことができる。

【0119】パリティビットを用いて鍵を選択する場合も、図3～図6で示した暗号化／復号方法と同様の効果を有しており、OSを介在させずに、計算量の少ない暗号化／復号方法を用いても十分な暗号強度を得ることができる。しかも、このパリティビットを用いて鍵を選択する方法では、暗号鍵及び復号鍵の選択に用いるビットを抽出する機構として一般のコンピュータシステムに標準的に用いられているパリティチェックの機構を利用している。そのため、その部分の機構を装置に新たに付加する必要がなく、装置構成を簡単にすることができる。

【0120】なお、パリティビットにより鍵を選択する場合においても、図7に示したように、鍵テーブル113を暗号化／復号アルゴリズム&鍵テーブル214に置き換えることにより、鍵と暗号化／復号のアルゴリズムとの組み合わせを選択することも可能である。このようにすることで複数の暗号化／復号のアルゴリズムを用いてプログラムやデータを暗号化することができ、計算量の少ない暗号化方式においても暗号強度を十分高くすることができる。

【0121】

【発明の効果】以上説明したように、情報処理装置に係る第1の発明では、暗号化されたデータそのものが識別データと暗号化対象データとに分離され、分離された識別データにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。。従って、情報処理装置で取り扱われるデータを複数の暗号方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、暗号化されるデータの一部を識別データとして用いているので、復号方式を特定するために余分な情報を付加する必要がなく、データサイズが増加することによる複雑なアドレス管理やメモリの浪費を避けることができ、一般のコンピュータシステムに適用する場合に極めて有効である。また、識別データの位置が解析され識別データが露呈した場合でも暗号方式そのものが露呈することはない、識別データの位置を固定とした場合でも暗号強度を十分強く保つことが可能である。これにより、暗号化データに対するランダムアクセスが可能となる。

【0122】また、情報処理装置に係る第2の発明では、暗号化データの関数値により暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合で

も暗号化強度の高い暗号化データを得ることができる。また、暗号化データに対するランダムアクセスも可能となる。

【0123】また、情報処理装置に係る第3の発明では、暗号鍵そのものではなく識別データを付加しているのでソフトウェア設計者に識別データのビット長を公開したとしても、暗号鍵そのもののビット長は秘密にすることができるので、暗号強度の低下を防ぐことができる。従って、この情報処理装置によれば、暗号化されているデータにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、暗号鍵そのものではなく識別データを用いることによって暗号鍵のビット長に制約がなくなる。また、識別データの位置が解析され識別データが露呈した場合でも暗号方式そのものが露呈することはなく、識別データの位置を固定とした場合でも暗号強度を十分強く保つことが可能である。これにより暗号化データに対するランダムアクセスが可能となる。

【0124】また、情報処理装置に係る第4の発明では、データのパリティビットをもとに暗号化方式又は復号方式を決定するので、プログラムやデータを複数の暗号化方式又は復号方式で暗号化して一つのメモリに格納しても、メモリのエリアごとの管理やアドレスごとの管理がまったく必要なくなるとともに、汎用のパリティチェック機構を暗号化方式又は復号方式の決定に利用することで、複数の暗号化方式又は復号方式の管理に必要な機構を大幅に削減することができる。従って大幅なコスト低減が可能となる。

【図面の簡単な説明】

【図1】本発明の暗号化復号装置の原理構成を示す図である。

【図2】本発明を実施するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。

【図3】図2に示される暗号化／復号装置の暗号化の処理手順を示すフローチャートである。

【図4】図3の各ステップの状態遷移を示す図である。
(A)はステップ1の状態を示す図であり、(B)はステップ2の状態を示す図であり、(C)はステップ3の状態を示す図であり、(D)はステップ4の状態を示す図であり、(E)はステップ5の状態を示す図である。

【図5】図2に示される暗号化／復号装置の復号の処理手順を示すフローチャートである。

【図6】図5の各ステップの状態遷移を示す図である。
(A)はステップ11の状態を示す図であり、(B)はステップ12の状態を示す図であり、(C)はステップ

13の状態を示す図であり、(D)はステップ14の状態を示す図であり、(E)はステップ15の状態を示す図である。

【図7】複数の暗号化及び復号のアルゴリズムを使用するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。

【図8】適当に選択した鍵を暗号鍵とする場合の処理手順を示すフローチャートである。

【図9】図8の各ステップの状態遷移を示す図である。

(A)はステップ21の状態を示す図であり、(B)はステップ22の状態を示す図であり、(C)はステップ23の状態を示す図であり、(D)はステップ24の状態を示す図である。

【図10】ハッシュ関数を用いて暗号化データと暗号鍵とを対応付ける場合の処理手順を示すフローチャートである。

【図11】図10の各ステップの状態遷移を示す図である。
(A)はステップ31の状態を示す図であり、

(B)はステップ32の状態を示す図であり、(C)はステップ33の状態を示す図であり、(D)はステップ34の状態を示す図であり、(E)はステップ35の状態を示す図である。

【図12】他の装置から提供される暗号化データを復号できるソフトウェアの保護機能付き情報処理装置を示すブロック図である。

【図13】本発明の情報処理装置の他の実施形態を示す図である。

【図14】パリティビットにより鍵を特定する暗号化方法のフローチャートである。

【図15】図14の各ステップの状態遷移図である。

(A)はステップ41の状態を示す図であり、(B)はステップ42の状態を示す図であり、(C)はステップ43の状態を示す図であり、(D)はステップ44の状態を示す図であり、(E)はステップ45の状態を示す図である。

【図16】パリティビットにより鍵を特定する復号方法のフローチャートである。

【図17】図16の各ステップの状態遷移図である。

(A)はステップ51の状態を示す図であり、(B)は、ステップ52の状態を示す図であり、(C)はステップ53の状態を示す図であり、(D)はステップ54の状態を示す図である。

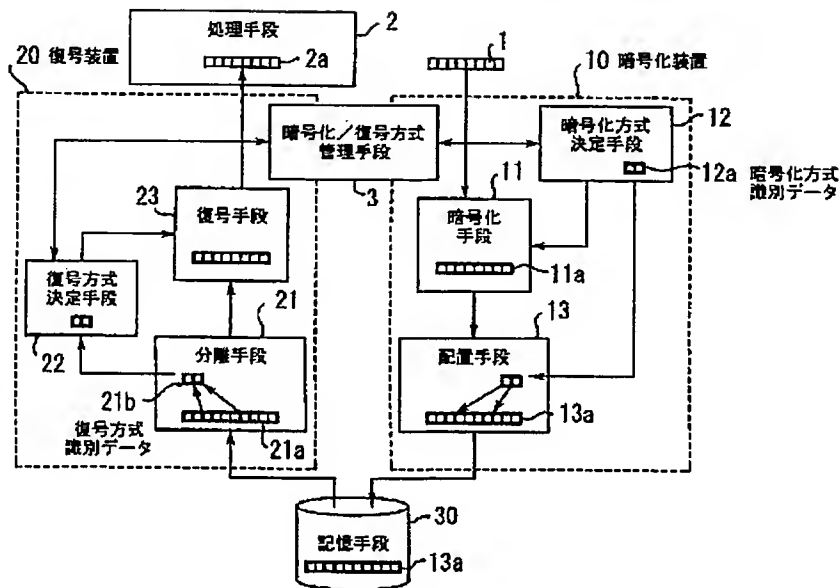
【図18】従来のソフトウェアの保護を図った情報処理装置のブロック図である。

【符号の説明】

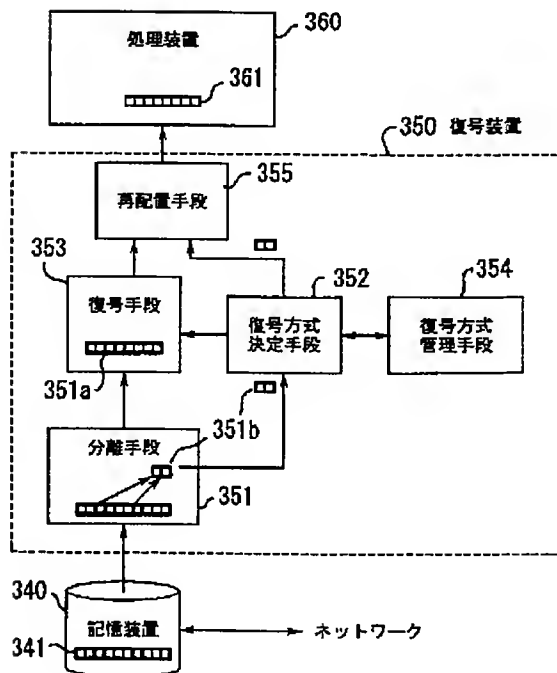
- 1 暗号化対象データ
- 2 処理手段
- 3 暗号化／復号方式管理手段
- 10 暗号化装置
- 11 暗号化手段

- | | |
|----------------|-----------------|
| 11a 暗号化データ | 22 復号方式決定手段 |
| 12 暗号化方式決定手段 | 23 復号手段 |
| 12a 暗号化方式識別データ | 111 MPU |
| 13 配置手段 | 112 暗号化／復号装置 |
| 13a 暗号化データ | 113 鍵テーブル |
| 20 復号装置 | 121 メインメモリ |
| 21 分離手段 | 122 I/Oインターフェース |
| 21a 復号対象データ | 123 補助メモリ |
| 21b 復号方式識別データ | 131 システムバス |

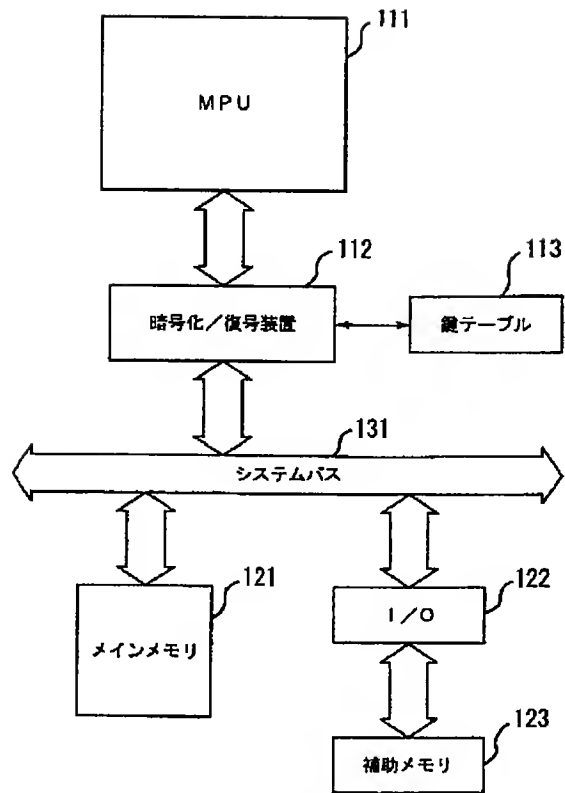
【図1】



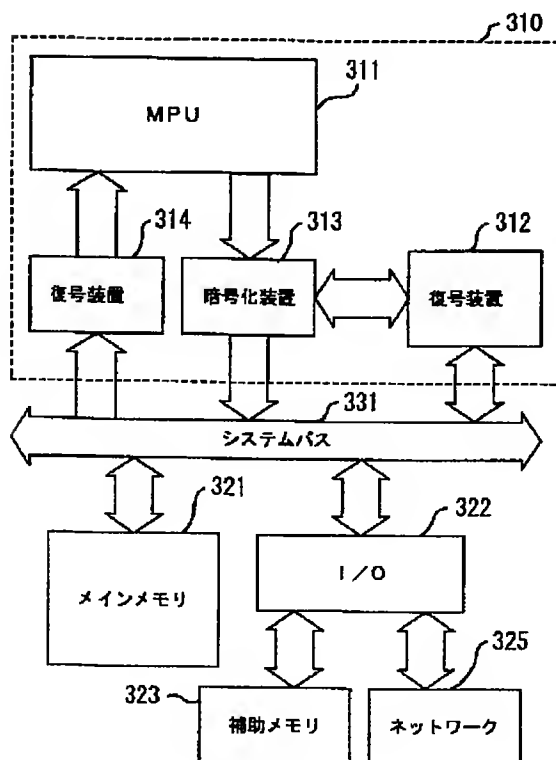
【図13】



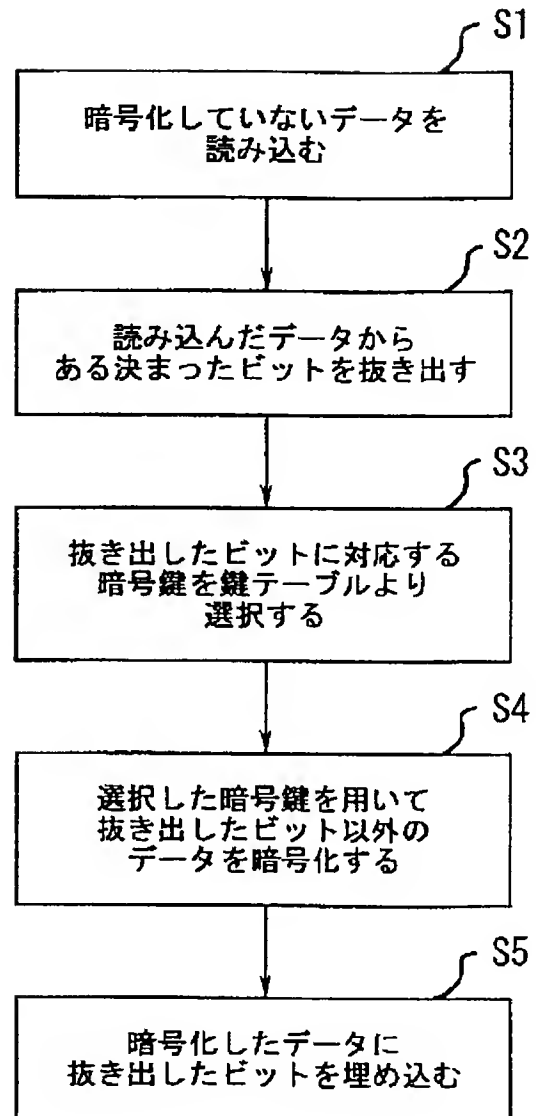
【図2】



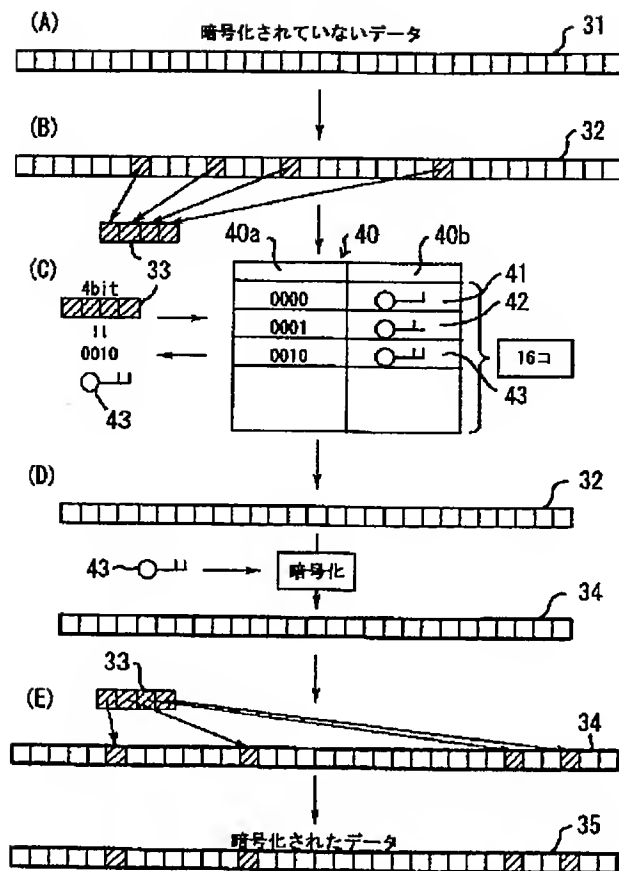
【図12】



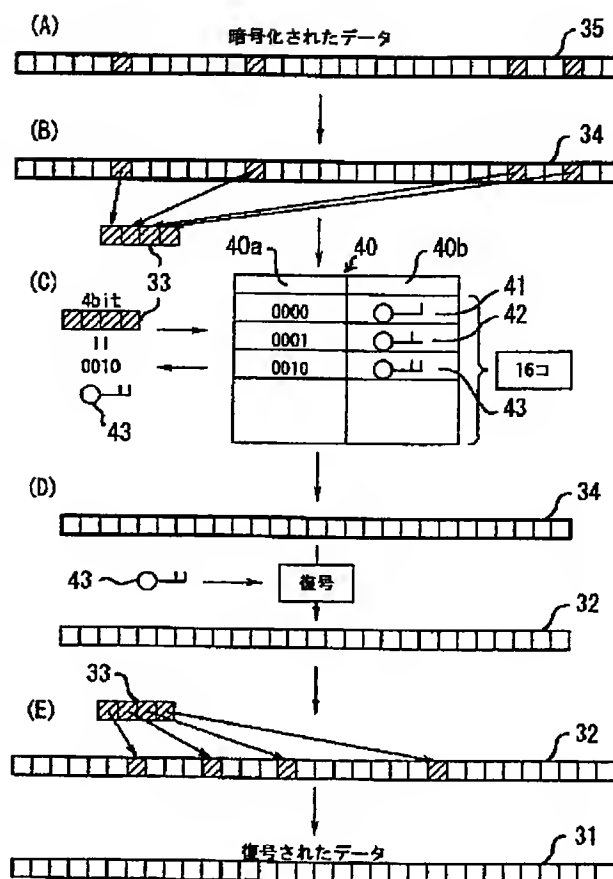
【図3】



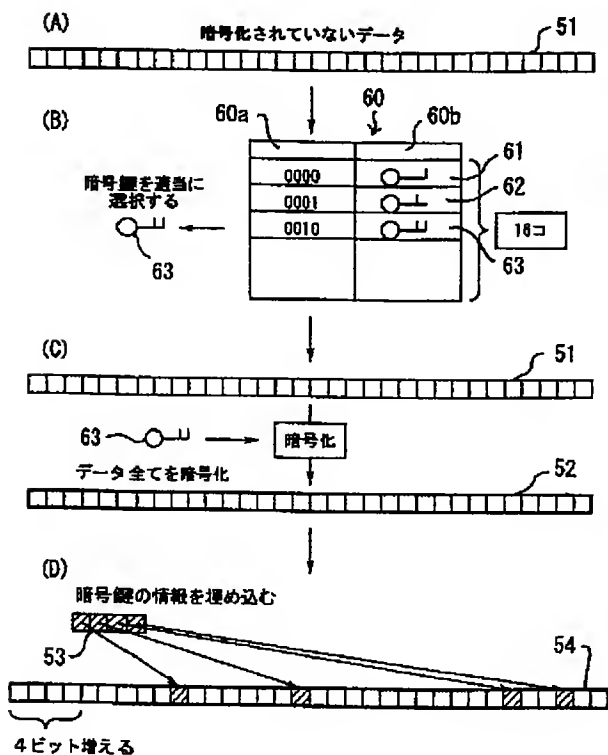
【图4】



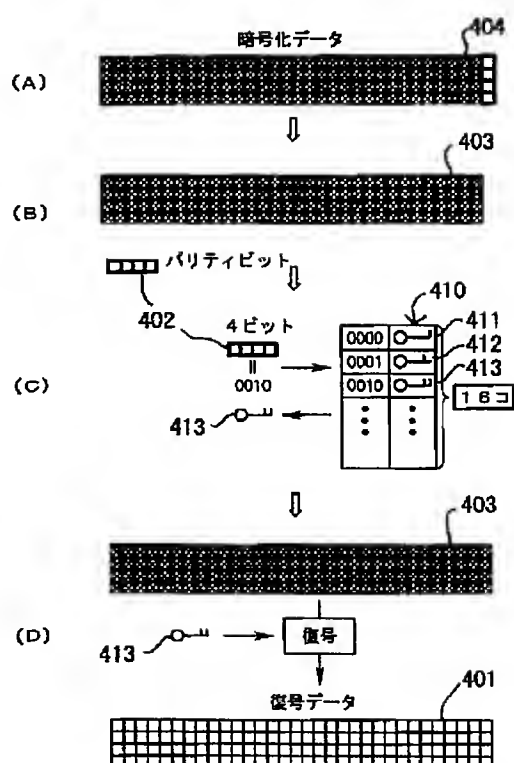
【図 6】



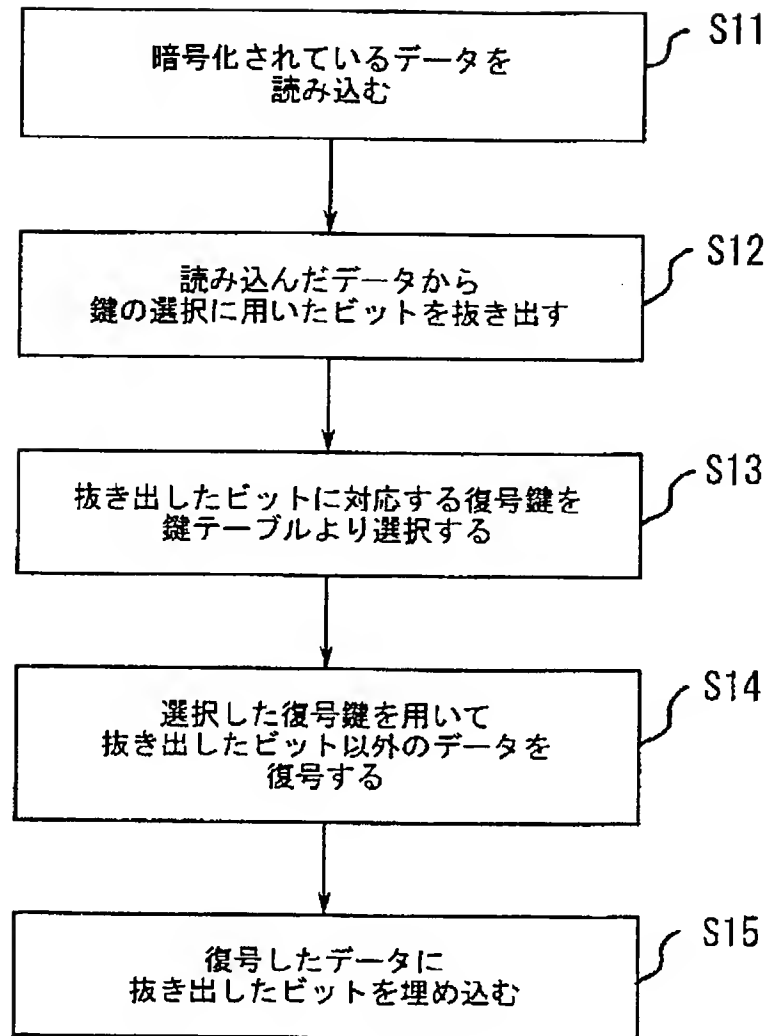
【図9】



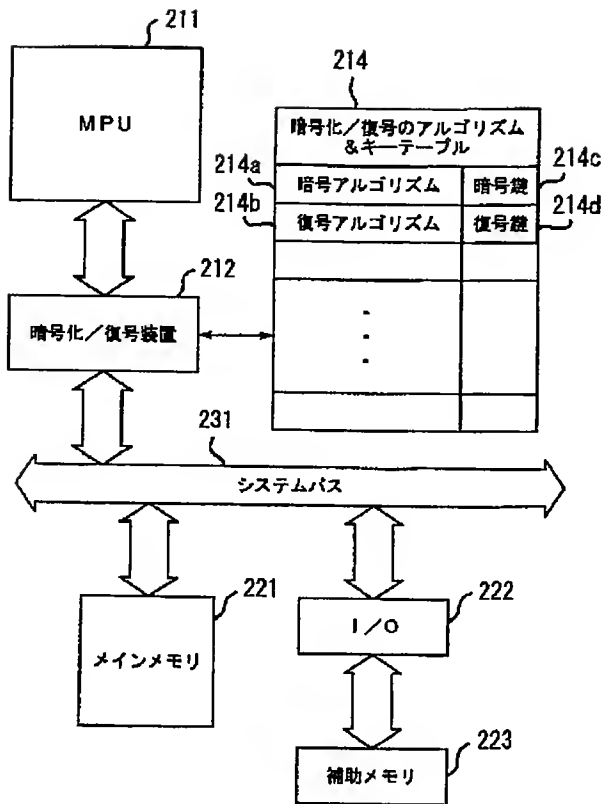
【图 17】



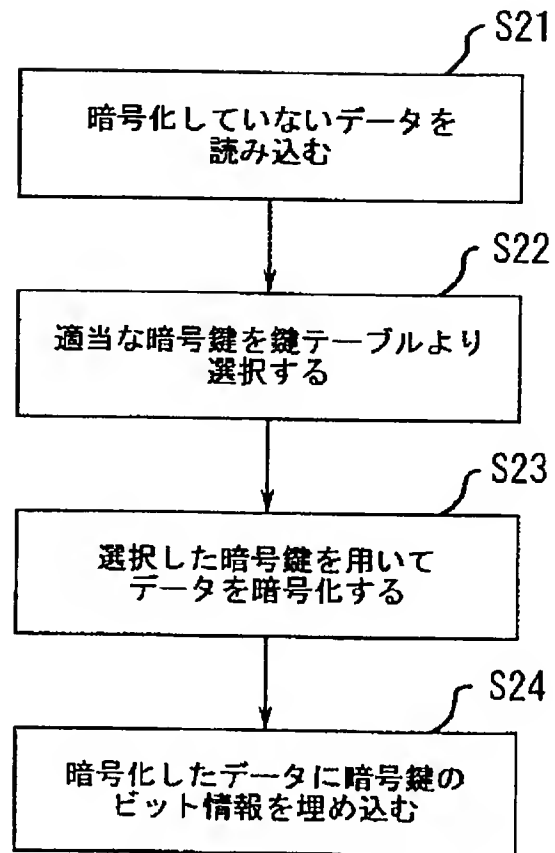
【図5】



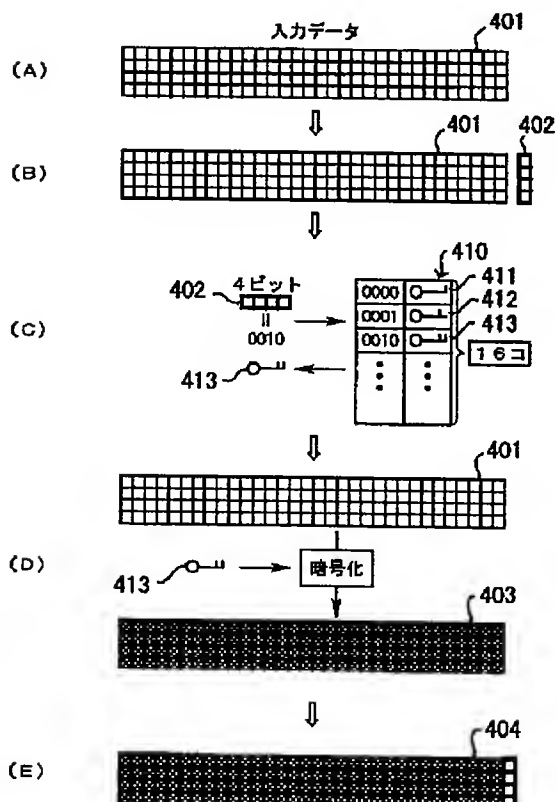
【図7】



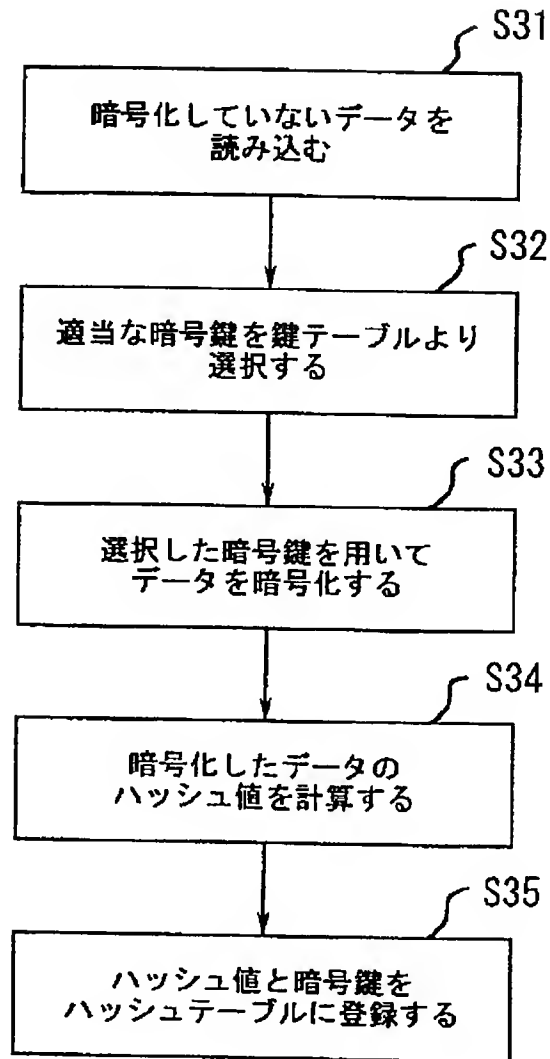
【図8】



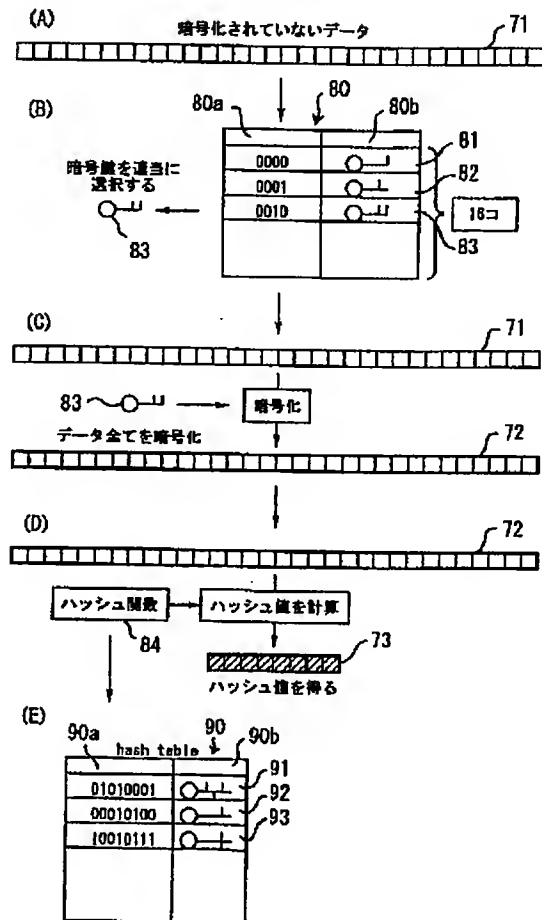
【図15】



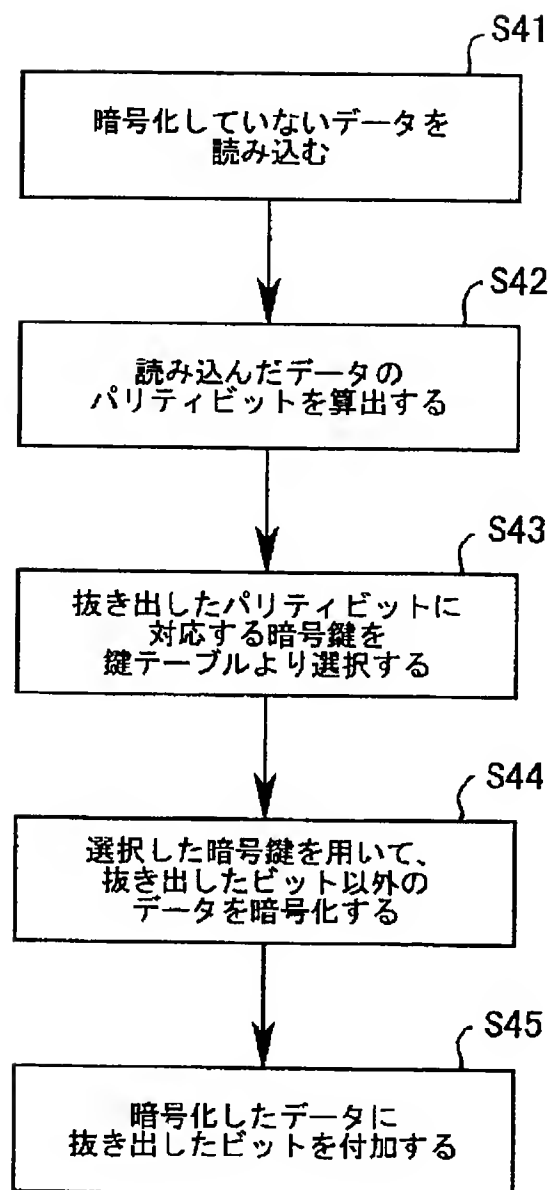
【図10】



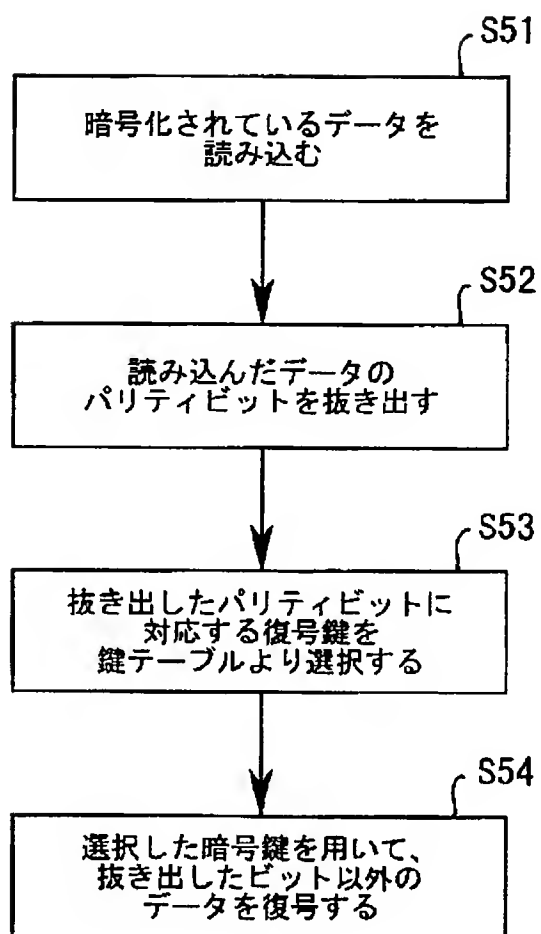
【図11】



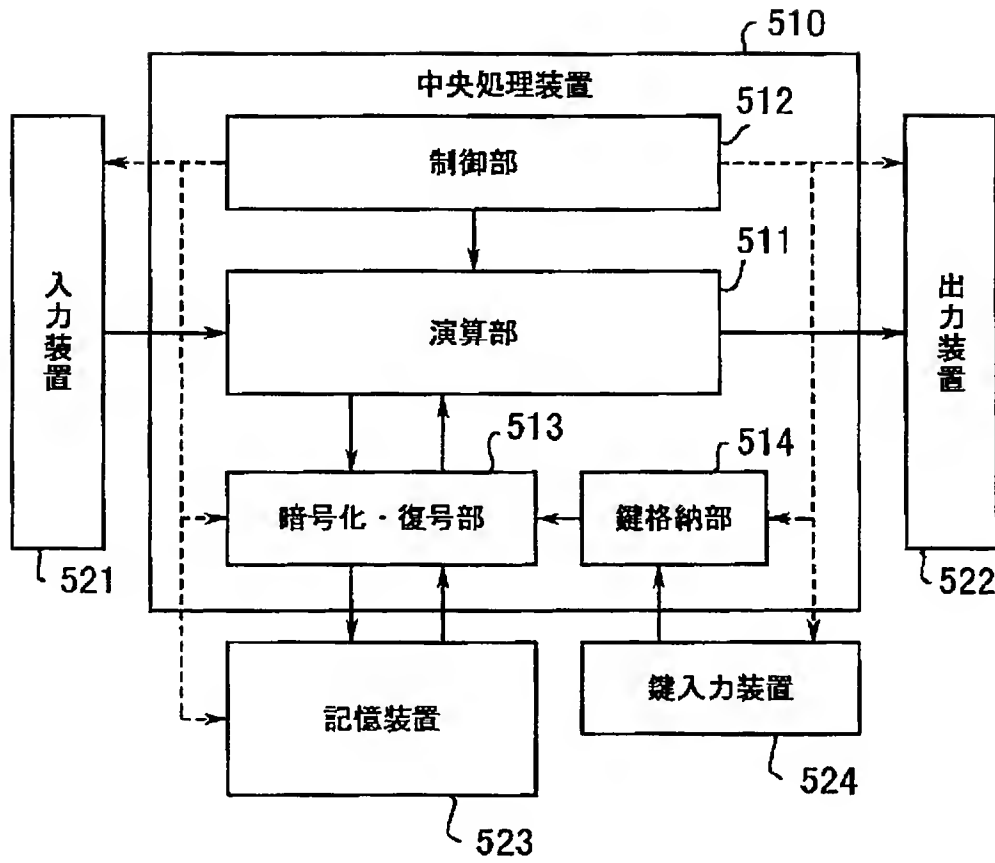
【図14】



【図16】



【図18】



【公報種別】特許法第17条の2の規定による補正の掲載
【部門区分】第7部門第3区分
【発行日】平成14年10月25日(2002.10.25)

【公開番号】特開平9-270785
【公開日】平成9年10月14日(1997.10.14)
【年通号数】公開特許公報9-2708
【出願番号】特願平8-180453
【国際特許分類第7版】

H04L 9/14
G09C 1/00 630
H04L 9/08

【F I】

H04L 9/00 641
G09C 1/00 630 B
H04L 9/00 601 B

【手続補正書】
【提出日】平成14年7月16日(2002.7.16)

【手続補正1】

【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】

【発明の名称】 情報処理装置及び情報処理方法

【手続補正2】

【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】

【請求項1】 入力されたデータを、識別データと暗号化対象データとに分離する分離手段と、
前記分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項2】 入力されたデータを暗号化する暗号化装置を有する報処理装置において、
暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する選択手段と、
前記選択手段により選択された暗号化方式を用いて前記入力されたデータを暗号化し、暗号化データを生成する

暗号化手段と、
前記暗号化手段により暗号化された暗号化データを、所定の関数に入力して関数値を計算する計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記計算手段により得られた関数値に対応付けて格納する復号方式記憶手段と、
を有することを特徴とする情報処理装置。

【請求項3】 暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項4】 前記暗号化手段を囲む包囲体に対して外部から物理的な作用を受けると、前記暗号化手段の処置機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項1、請求項2、又は請求項3のいずれか1項に記載の情報処理装置。

【請求項5】 前記決定手段により決定される暗号化方式を変更する変更手段をさらに有することを特徴とする請求項1、請求項2、又は請求項3のいずれか1項に記載の情報処理装置。

【請求項6】 識別データが復号対象データ内の所定の位置に配置された入力データを、前記識別データと前記復号対象データとに分離する分離手段と、
前記分離手段が分離した前記識別データに応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、
前記決定手段で決定された復号方式を用いて、前記復号

対象データを前記復号対象データと同ビット数に復号する復号手段と、

前記識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項7】 入力された暗号化データを復号する復号装置を有する情報処理装置において、
前記暗号化データを、所定の関数に入力して関数値を計算する計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記関数値に対応づけて格納する復号方式記憶手段と、
前記計算手段により算出された関数値に対応する復号方式を前記復号方式記憶手段内から選択する復号方式選択手段と、
前記復号方式選択手段で選択された復号方式を用いて、前記暗号化データを復号する復号手段と、
を有することを特徴とする情報処理装置。

【請求項8】 前記復号手段を囲む包囲体に対して外部から物理的な作用を受けると、前記復号手段の処理機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項6又は請求項7のいずれか1項に記載の情報処理装置。

【請求項9】 前記決定手段により決定される復号方式を変更する変更手段を、さらに有することを特徴とする請求項6又は請求項7のいずれか1項に記載の情報処理装置。

【請求項10】 データの暗号化及び暗号化データの復号を行う暗号化装置及び復号装置を有する情報処理装置において、

入力されたデータを、識別データと暗号化対象データとに分離する入力データ分離手段と、

前記入力データ分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、
前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、

前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、

前記配置手段により前記識別データが配置された暗号化データを格納する記憶手段と、

前記記憶手段に格納された前記識別データが配置された暗号化データを、識別データと暗号化データとに分離する分離手段と、

前記分離手段により分離された識別データに応じて、暗号化方式に対応した復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決

定手段と、

前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを前記暗号化データと同ビット数に復号する復号手段と、

前記復号方式決定手段による復号方式を示す識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する再配置手段と、

前記復号手段により復号されたデータの処理を行う情報処理手段と、

を有することを特徴とする情報処理装置。

【請求項11】 データの暗号化及び暗号化データの復号を行う暗号化復号装置を有する情報処理装置において、

暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する暗号化方式選択手段と、

前記暗号化方式選択手段により選択された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化手段により暗号化された暗号化データを、特定の関数に入力して関数値を計算する第1の計算手段と、

前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記第1の計算手段により得られた関数値に対応づけて格納する復号方式記憶手段と、

前記暗号化手段により暗号化された暗号化データを格納する記憶手段と、

前記記憶手段に格納された暗号化データを、特定の関数に入力して関数値を計算する第2の計算手段と、

前記第2の計算手段により算出された関数値に対応する復号方式を、前記復号方式記憶手段内から選択する復号方式選択手段と、

前記復号方式選択手段で選択された復号方式を用いて、

前記暗号化データを復号する復号手段と、

前記復号手段により復号されたデータの処理を行う情報処理手段と、

を有することを特徴とする情報処理装置。

【請求項12】 予め復号鍵と復号アルゴリズムとが特定されている暗号化データが入力されると、入力された暗号化データを復号する既知方式復号手段をさらに有し、

前記暗号化手段は、前記既知方式復号手段で復号されたデータも、暗号化対象データとして暗号化することを特徴とする請求項2、請求項3、請求項10、又は請求項11のいずれか1項に記載の情報処理装置。

【請求項13】 入力された暗号化データが暗号化された際の暗号化方式と異なる暗号化方式により、前記復号手段が復号したデータを暗号化する別方式暗号化手段を、さらに有することを特徴とする請求項6、請求項7、請求項10、又は請求項11のいずれか1項に記載

の情報処理装置。

【請求項14】 入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、

前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化する暗号化手段と、
を有することを特徴とする情報処理装置。

【請求項15】 復号対象データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、

前記決定手段で決定された復号方式を用いて、前記復号対象データを復号する復号手段と、
を有することを特徴とする情報処理装置。

【請求項16】 入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、

前記暗号化方式決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化手段により生成された前記暗号化データを格納する記憶手段と、

前記記憶手段内に格納された前記暗号化データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する復号方式決定手段と、
前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、

を有することを特徴とする情報処理装置。

【請求項17】 入力されたデータを、識別データと暗号化対象データとに分離し、

分離した識別データに応じて、暗号鍵と暗号化アルゴリ

ズムの組み合わせにより特定される暗号化方式を決定し、

決定された暗号化方式を用いて前記暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成し、

前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置することを特徴とする情報処理方法。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正内容】

【0001】

【発明の属する技術分野】本発明はソフトウェアの保護機能付情報処理装置及び情報処理方法に関し、特に処理が行われたデータを逐次暗号化する暗号化装置を有するか、処理を行うべき暗号化データを逐次復号する復号装置を有するか、あるいはそれらの双方を有する情報処理装置及び情報処理方法に関する。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0029

【補正方法】変更

【補正内容】

【0029】本発明はこのような点に鑑みてなされたものであり、コンピュータのメモリの管理方法に依存せず、少ない計算量の暗号アルゴリズム及び簡単な鍵管理により暗号強度の高い暗号化データを得る暗号化装置を有する情報処理装置及び情報処理方法を提供することを目的とする。